Card edit

Important Yubico has learned of a security issue with the OpenPGP Card applet project that is used in the YubiKey NEO. This vulnerability applies to you only if you are using OpenPGP, and you have the OpenPGP applet version 1.0.9 or earlier. SecurityAdvisory 2015-04-14 (https://developers.yubico.com/ykneo-openpgp/SecurityAdvisory%202015-04-14.html)

Introduction

To configure the OpenPGP application on a YubiKey you can use GnuPG (https://www.gnupg.org).

The documentation in this section assumes the reader has a general understanding of how GnuPG works. For more in-depth documentation see the GnuPG documentation (https://www.gnupg.org/documentation/), especially the parts on the usage and setting of the PIN and reset codes may be useful.

Prerequisites

Installed the Yubikey personalization tool (https://developers.yubico.com/yubikey-personalization/Manuals/ykpersonalize.1.html).

Verify that your YubiKey has a firmware version 3.1.8 or later.

```
$ lsusb -v
...
```

Make sure that your device is in OTP/CCID or CCID mode, you can use ykpersonalize to switch to OTP/U2F/CCID:

```
$ ykpersonalize -m6
...
```

Check that your libccid version is 1.4.10 or later so that /etc/libccid_Info.plist contains the YubiKey USB PID/VID.

Check that your PCSCD setup is working. Use "pcsc_scan" to check for card readers, it should show "Yubikey" somewhere in the output.

You need to use the GnuPG agent with scdaemon, and we recommend using version 2.0.22 or later for full functionality.

To check the application version you may run, after inserting your YubiKey:

```
$ gpg-connect-agent --hex "scd apdu 00 f1 00 00" /bye
D[0000]  01 00 05 90 00                                     .....
OK
```

Where "01 00 05" means version 1.0.5. (see security advisory above if version < 1.0.10)

Note that with the release of YubiKey 4, this number will always be equal to the firmware version.

YubiKey 4 touch

YubiKey 4 introduces a new *touch* feature that allows to protect the use of the private keys with an additional layer. When this functionality is enabled, the result of a cryptographic operation involving a private key (signature, decryption or authentication) is released only if the correct user PIN is provided **and** the YubiKey touch sensor is triggered. This request of user presence ensures that no malware can issue commands to the YubiKey without the user noticing.
The YubiKey signals a request for a touch event by blinking for up to 15 seconds. If no touch is provided within this period, the operation will fail.

There are three possible values for the touch parameter:

off touch is disabled;

on touch is enabled;

fix touch is enabled and can not be disabled unless a new private key is generated or imported.

The touch parameter can be individually set on each one of the three private keys and requires the use of the admin PIN.

In order to activate this functionality, it is necessary to use a custom bash script called yubitouch.sh (https://github.com/a-dma/yubitouch).

Example

The following demonstrate setting all the parameters in the OpenPGP applet on a YubiKey.

```
user@debian:~$ gpg --card-edit

Application ID ...: D2760001240102000060000000420000
Version ..........: 2.0
Manufacturer .....: unknown
Serial number ....: 00000042
Name of cardholder: [not set]
Language prefs ...: [not set]
Sex ..............: unspecified
URL of public key : [not set]
Login data .......: [not set]
Signature PIN ....: forced
Key attributes ...: 2048R 2048R 2048R
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 3 3
Signature counter : 0
Signature key ....: [none]
Encryption key....: [none]
Authentication key: [none]
General key info..: [none]

gpg/card> admin
Admin commands are allowed

gpg/card> passwd
gpg: OpenPGP card no. D2760001240102000060000000420000 detected

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 3
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 1
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? q
```

```
gpg/card> name
Cardholder's surname: Josefsson
Cardholder's given name: Simon

gpg/card> lang
Language preferences: sv

gpg/card> url
URL to retrieve public key: https://josefsson.org/1c5c4717.txt

gpg/card> sex
Sex ((M)ale, (F)emale or space): m

gpg/card> login
Login data (account name): jas

gpg/card>

Application ID ...: D2760001240102000060000000420000
Version ..........: 2.0
Manufacturer .....: unknown
Serial number ....: 00000042
Name of cardholder: Simon Josefsson
Language prefs ...: sv
Sex ..............: male
URL of public key : https://josefsson.org/1c5c4717.txt
Login data .......: jas
Signature PIN ....: forced
Key attributes ...: 2048R 2048R 2048R
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 3 3
Signature counter : 0
Signature key ....: [none]
Encryption key....: [none]
Authentication key: [none]
General key info..: [none]

gpg/card> quit
user@debian:~$
```

The following example is YubiKey 4 specific and shows how to set touch on the signature key:

```
$ ./yubitouch.sh sig on
All done!
```

OATH (/OATH)

PGP (/PGP)

PIV (/PIV)

YubiHSM2 (/YubiHSM2)

Software Projects (/Software_Projects)

RESOURCES

Buy YubiKeys (https://www.yubico.com/store/)

Blog (https://www.yubico.com/blog/)

Newsletter (https://www.yubico.com/newsletter/)

Yubico Forum Archive (https://forum.yubico.com/)

YUBICO.COM (https://www.yubico.com/)

Why Yubico (https://www.yubico.com/why-yubico/)

About Yubico (https://www.yubico.com/about/about-us/)

(https://www.facebook.com/Yubikey) (https://www.youtube.com/c/Yubico) (https://github.com/Yubico)