Säkrare SSH med Yubikey

Viktor Ahlqvist

2020-02-07

Omegapoint kompetensdag

Målbild

- Inga nycklar på datorn
- Möjlighet att ta med nycklarna
- Möjliggör lättare backup, skriptad installation, ...

Open PGP nycklar

- Master key
  - Skapa nycklar
  - Signera/certifiera nycklar
  - Visa att du äger nycklar
- Subkeys
  - Används för signering, kryptering och/eller authentisering
  - Nycklarna som används vardagligen
- Nycklar kan genereras på Yubiken eller tas in

Konfigurera Yubikeyn

- Konfigurera med Yubikey manager (ykman)
- Stäng av OTP

  ```
  $ ykman config usb --disable OTP
  ```

- Aktivera touch

  ```
  $ ykman openpgp set-touch aut on
  ```

- Byt pin

  ```
  $ gpg --change-pin
  ```

Generera nycklar

- Generera på Yubikey eller för in nyckel
  Omöjligt (?) att föra ut privat nyckel
- Generera nycklar
  `generate`
- Om intresse: byt nyckeltyp/längd
  `key-attr`

```
$ gpg --card-edit
Reader ...........: 1050:04
…
gpg/card> admin
…
gpg/card> key-attr
…
gpg/card> generate
```

För SSH: GPG agent

- GPG agenten för SSH agenten
- *pinentry* program för att mata in pinkoden
- `$ ssh-add -L` bör visa en `cardno:`-nyckel
- Ladda upp på Github (eller motsv)
- Testa med `$ ssh -v git@github.com`

Signera commits i Git

- Lista kända nycklar

  ```
  $ gpg --list-secret-keys --keyid-format LONG
  ```

- Exportera publika nyckeln

  ```
  $ gpg --armor --export KEYID
  ```

- Ladda upp på Github (eller motsv)
- Konfigurera git att använda en specifik nyckel

  ```
  $ git config --global user.signingkey KEYID
  ```

- Signera commits med `-S` och taggar med `-s`

  ```
  $ $ git commit -S -a -v
  $ git tag -a '1.0.0' -m 'First release' -s
  ```

Källor

- drduhs Yubikey-Guide https://github.com/drduh/YubiKey-Guide/
- Debians information om subkeys: https://wiki.debian.org/Subkeys
- esev https://www.esev.com/blog/post/2015-01-pgp-ssh-key-on-yubikey-neo/
- florin (Mac OS) https://florin.myip.org/blog/easy-multifactor-authentication-ssh-using-yubikey-neo-tokens
- ixdy (tillägg till florin) https://gist.github.com/ix-dy/6fdd1ecea5d17479a6b4dab4fe1c17eb