**Multi-Factor Authentication**

**Something you know**

* **Authentication by knowledge**
  + Passwords, PINs etc.

**Something you have**

* **Authentication by ownership**
  + ID, credit card, soft token (google authenticator), hardware token (YubiKey/NitroKey), SMS or email

**Something a person is**

* **Authentication by characteristic**
  + Retina Scan, Thumb scan, Biometrics

Soft token

* The ‘something you have’ is generated in software

**Authy**

* Offline syncing (no cloud service)
* Multiple devices for 2FA
  + Must use multiple devices with second token on or you could lose access to it

**Hard Tokens**

**Dongle**

* **DigiFlak**
* **NitroKey**
* **VASCO**
* **WWPass**
* **Yubico**

**Twofactprauth.org**

* Tells you what 2fa websites use

Yubikey neo with NFC for android

Also works for whole disk encryption

Works with VeriCrypt and other crypto systems with a customisable tool kit

With SMS for example, phones can be hacked or MITM attacks to receive your SMS authentication

* Better than nothing but not as good as hard tokens

**The Future of Password Authentication**

* Will slowly fade away and be replaced
* SQRL
* Clef