Making an "Open Everything" Password Safe

anelok.com

Werner Almesberger
werner@almesberger.net

The problem

- Digital life is full of passwords
- Passwords aren't going away
- (Some) should be difficult to guess/crack . . .
  . . . but easy to remember
- Keep them . . .
  - in your wallet ?
  - on your smartphone ?
  - in the Cloud (single sign-on) ?
- Not all interfaces are open or online

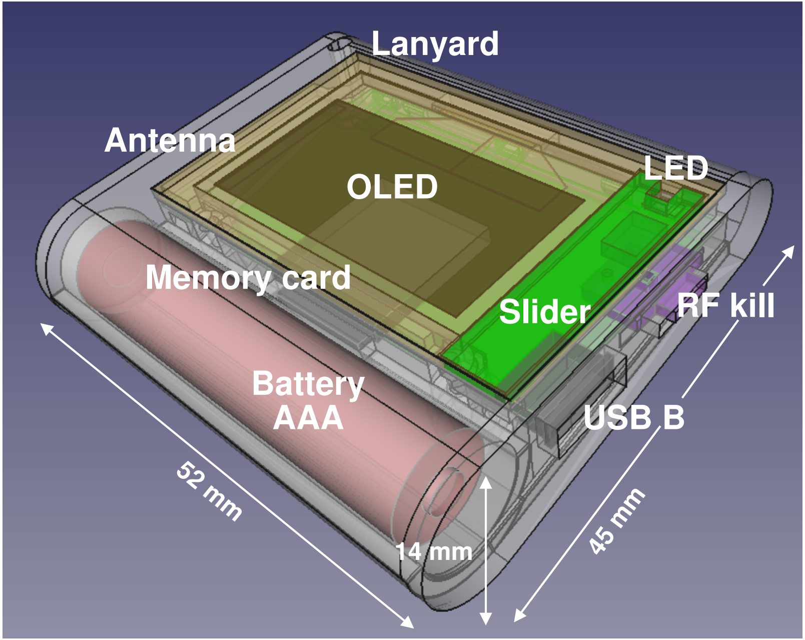
Enter Anelok

Use cases:

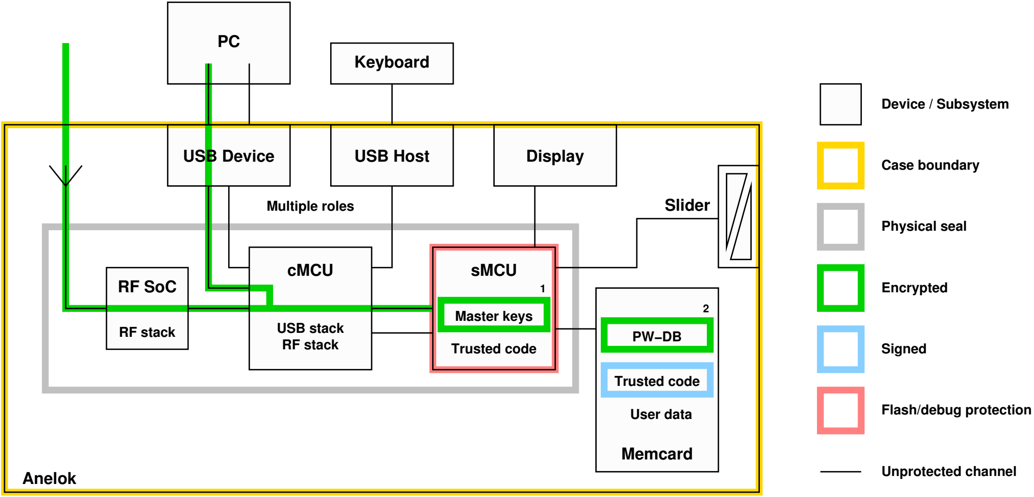
- Remember passwords for human use
- Manage “hardened” passwords and protocols
- Both for legacy and all-digital scenarios

Design properties:

- Personal and portable
  → the size of a cigarette lighter
- Single function
  → reduced attack surface
- Open . . . Software, Hardware, Tools, Development
  → can be reviewed, adapted, fixed


Lanyard
Antenna
OLED
LED
Memory card
Slider
RF kill
Battery
AAA
USB B
52 mm
14 mm
45 mm

Anelok security model (basic, 2015 design)



[1] Encrypted with PIN (weak), retry limit for device unlocking

[2] Per–object symmetric encryption, object keys encrypted with master keys

Would you like to know more ?

- Web: `anelok.com`
- Village: at the **Neo** village