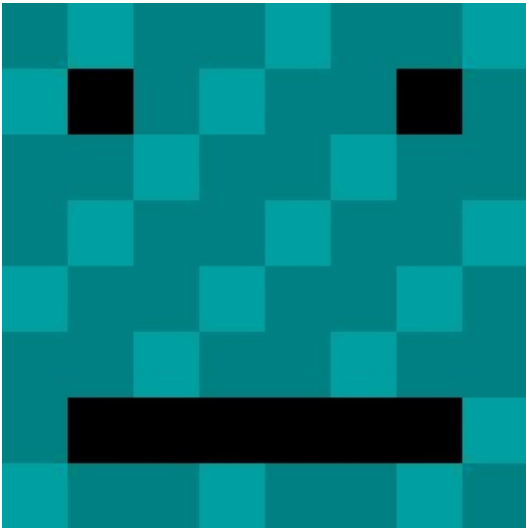


Implanting hardware as a hobby

About



Juha Kivekäs

@_guttula

Almost BS of CS

Security Consultant at F-Secure

Hardware, Crypto, Minimalism

Structure

Overview of Implants
Vulnerability
Sniffer Implant
Attack Scenario

Implants

Hardware Implants

- Nasty pieces of hardware added to a device
- Keyloggers
- Credit card skimmers
- Modified/Trojaned chips

- Not implants in humans or animals

Implant Lifecycle

- Attachment
- Manipulation or Sniffing
- Exfiltration or Recovery



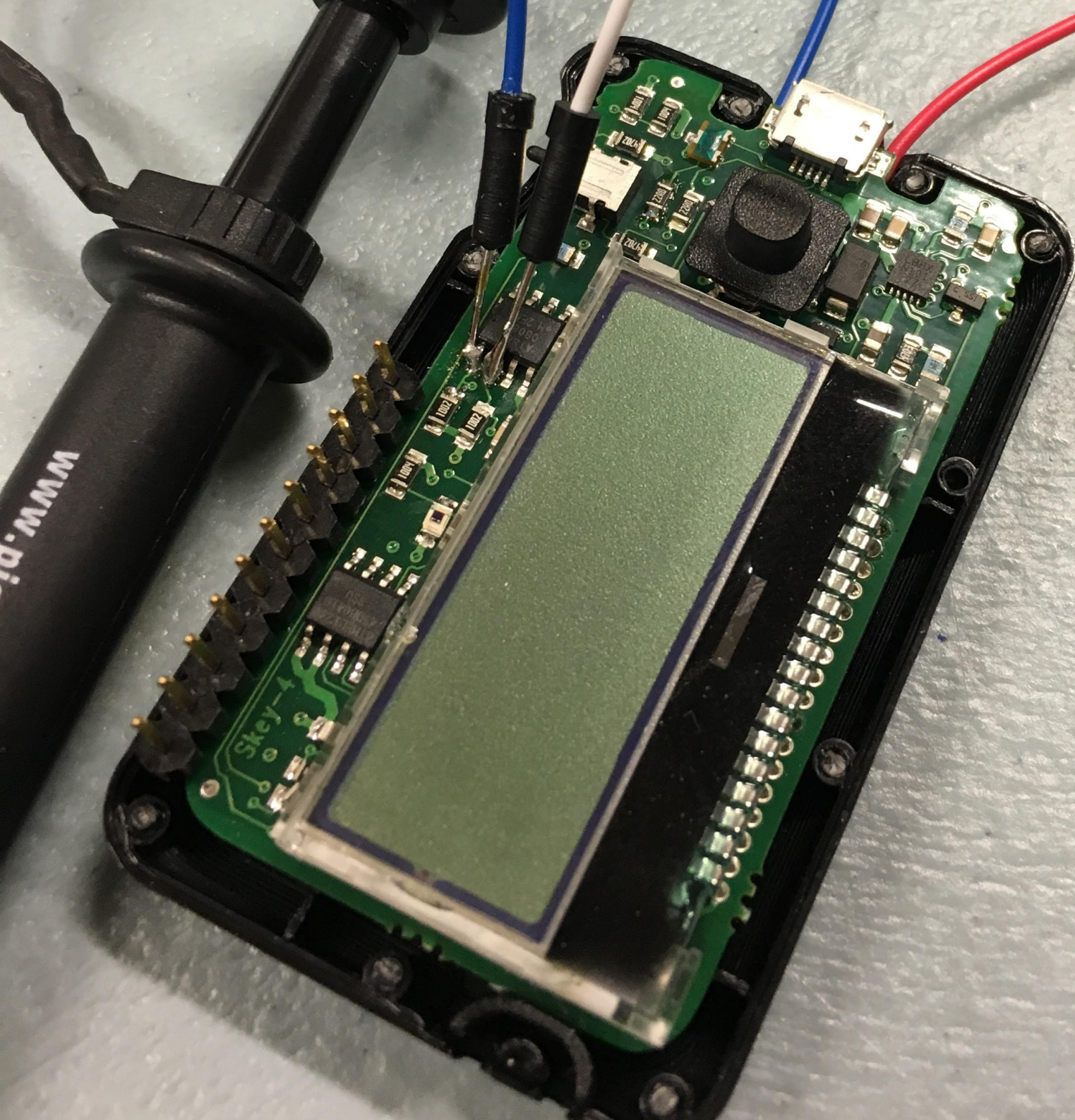
Vulnerability



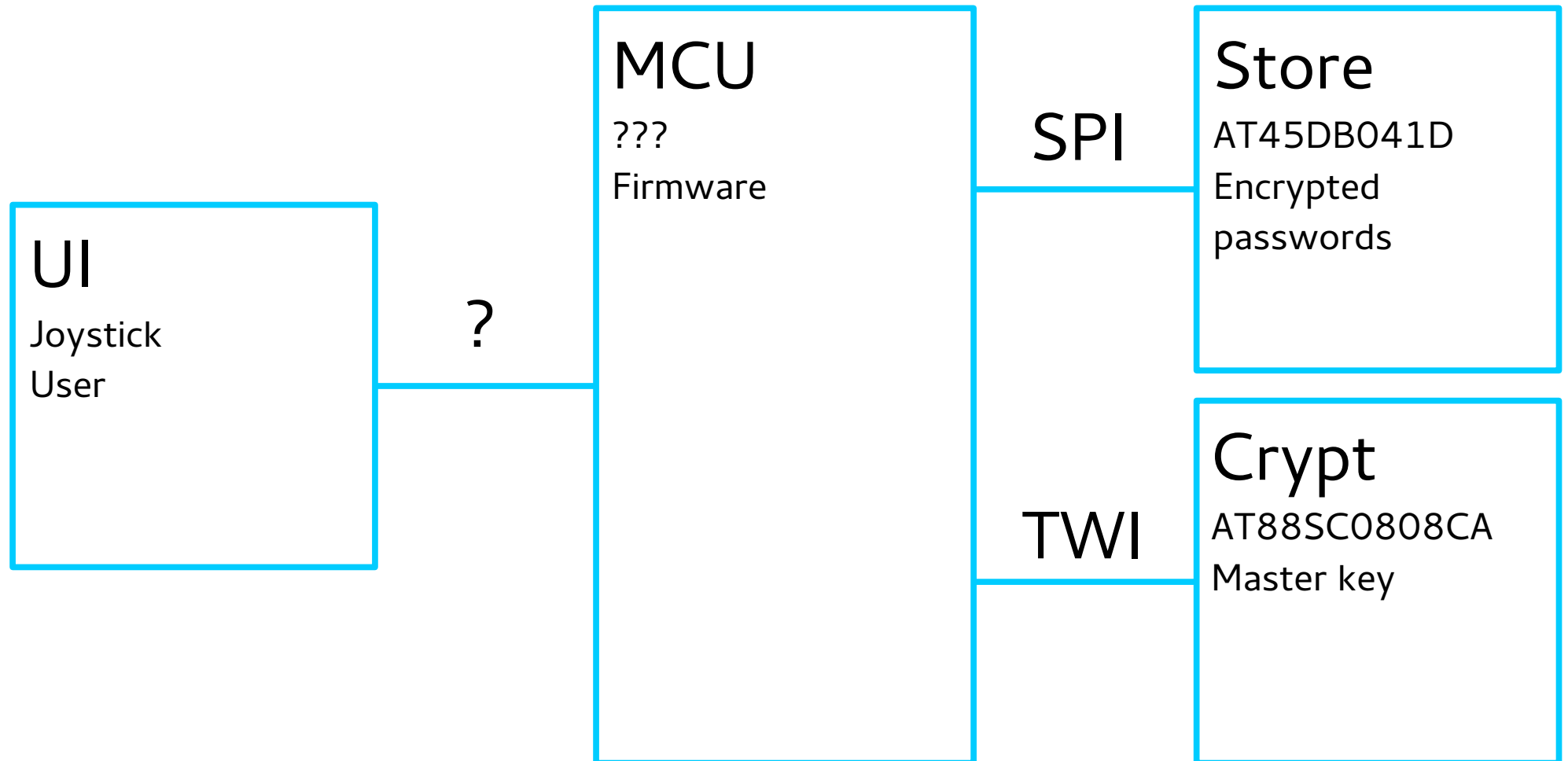
The Target Device: Seclave

- Hardware password manager
- Engineers user interface
- <http://www.seclave.se/>



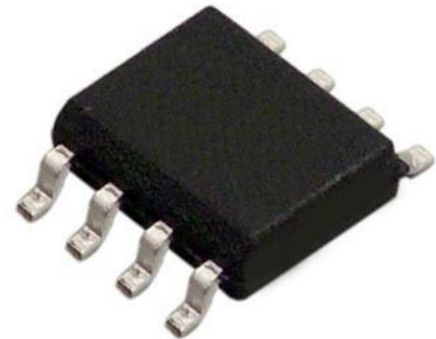


Hardware layout



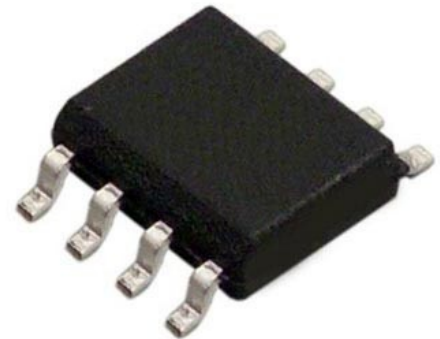
The Store: AT45DB041D

- It's a flash chip
(Full of juicy passwords)



The Crypt: AT88SC0808CA

- Data in rest that cannot be read or modified
- Tamper proof storage
- Password protected
- Three bytes
- Four tries

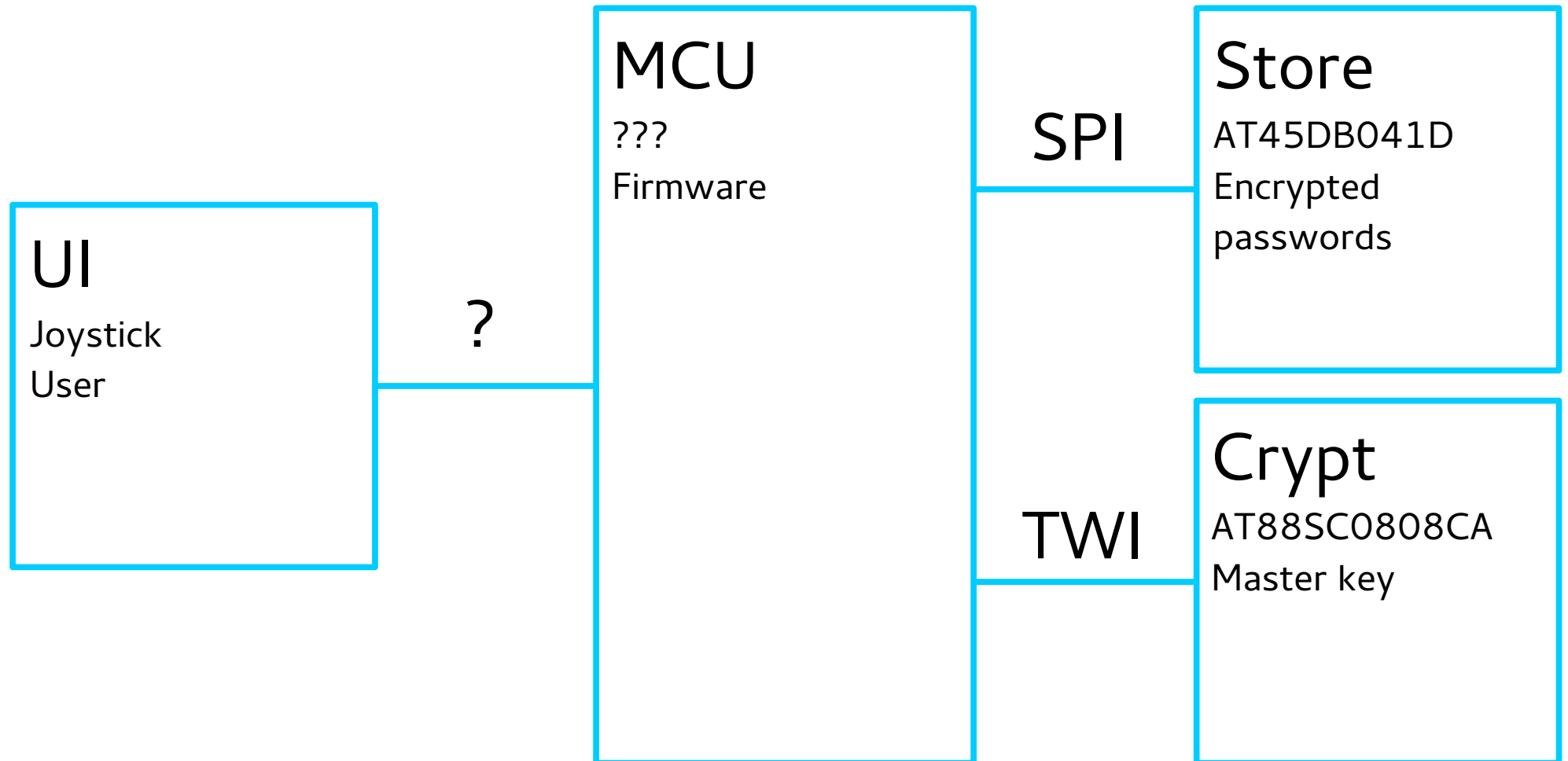


The MCU: some Atmel AVR

- It's under the screen
- I never looked

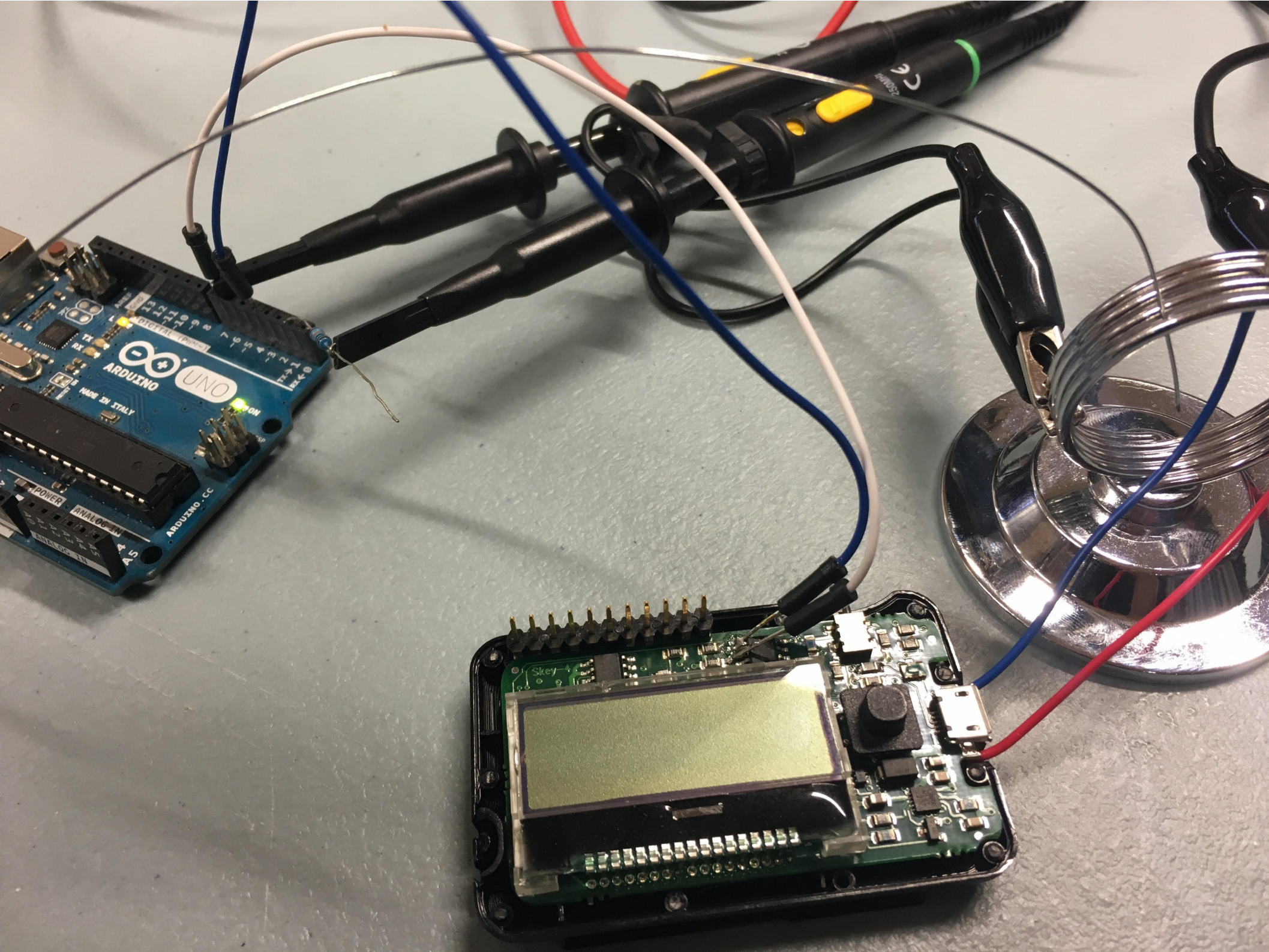


Hardware layout

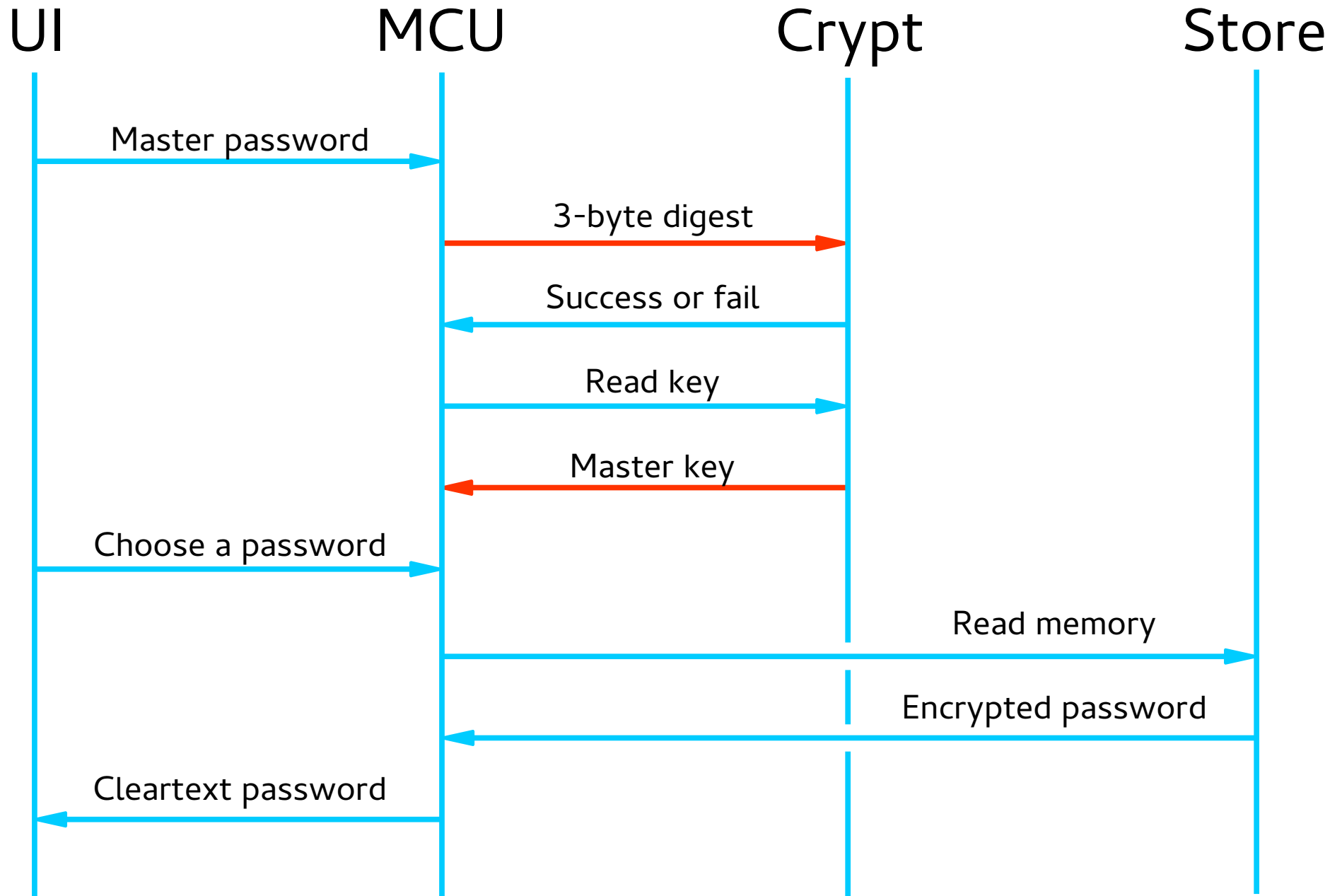


TWI / I²C

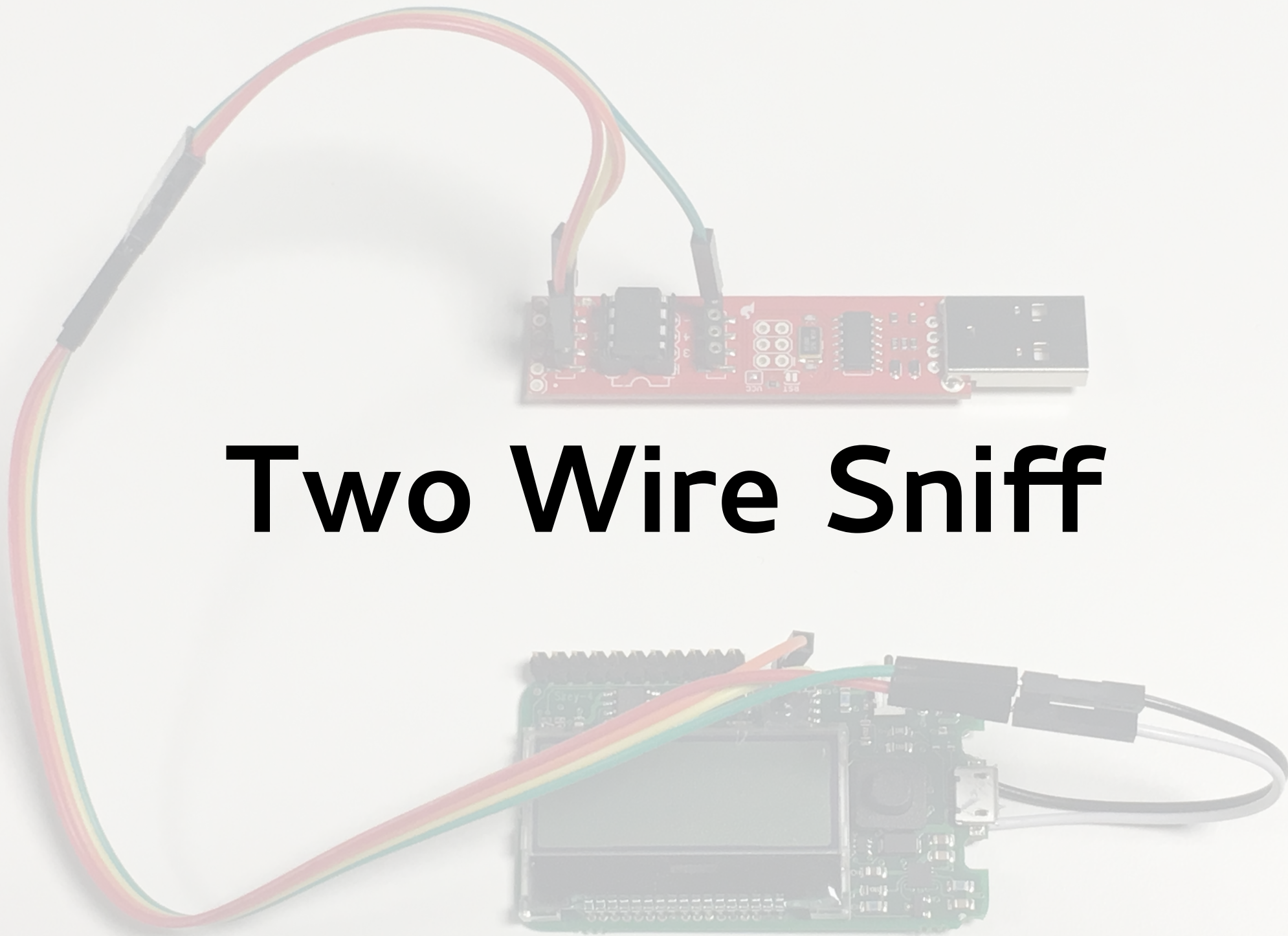
- Two Wire Interface / Inter-Integrated Circuit
- Physical layer
- Simple byte transfer protocol
- Primary - Replica



Sequence diagram

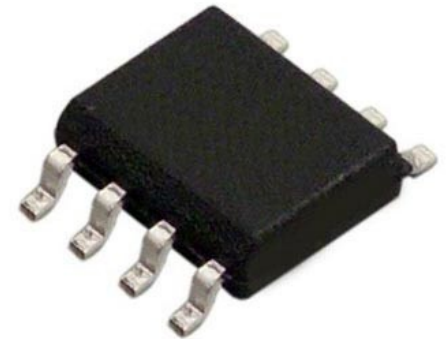


Two Wire Sniff



Two Wire Sniff: ATTINY4520PU

- Hardware for TWI communication
- EEPROM for non-volatile storage
- Cheap, 2€



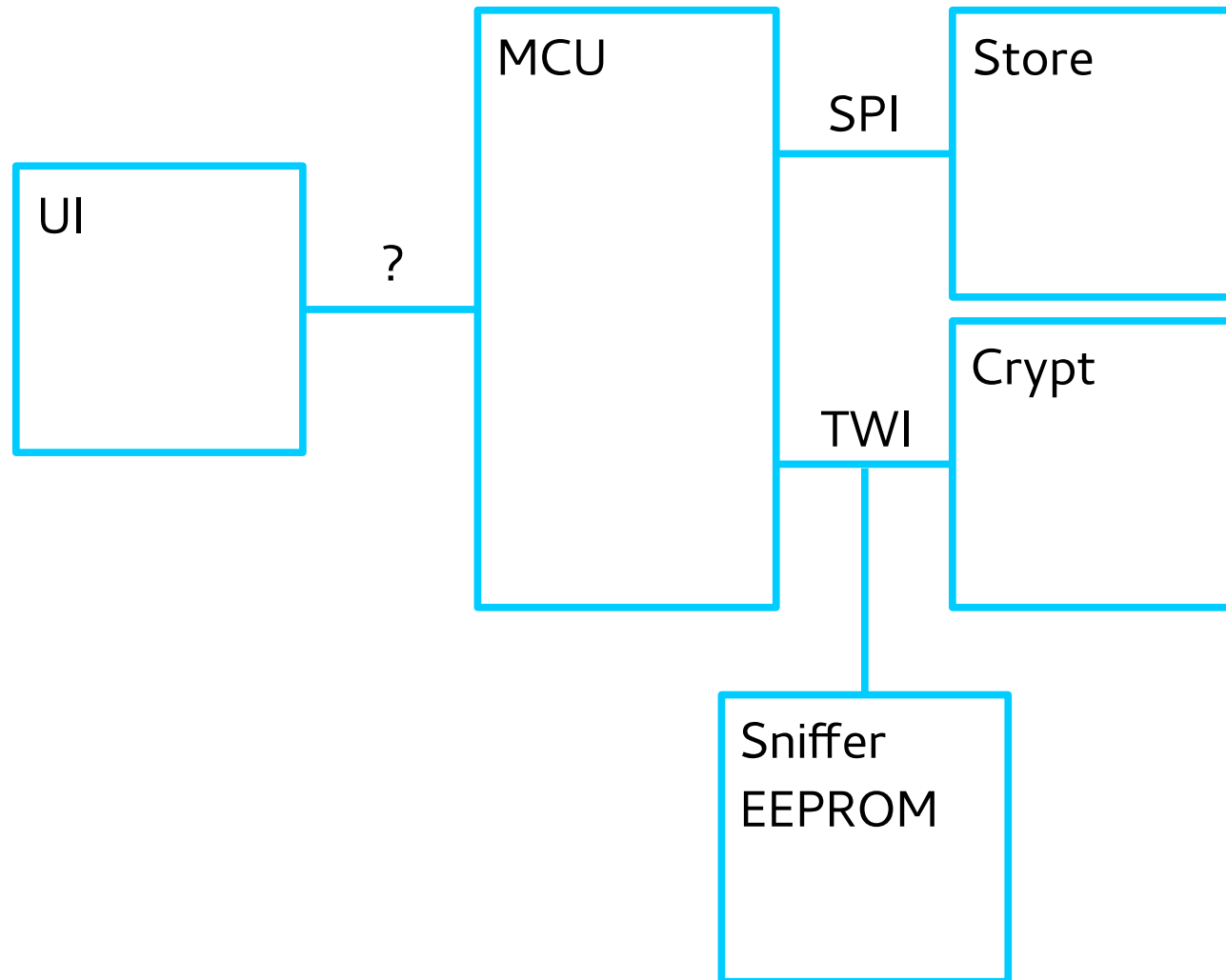
Two Wire Sniff

- Connected to target SDA, SCL, VCC, and GND
- EEPROM can be read via programming device
- Less than 1k code

Two Wire Sniff

- Sits on the TWI bus and listens to everything
- Stores the bus data in RAM
- Moves the data from RAM to EEPROM

Hardware layout





Backup key
8F23743E CE16EA67

[illegible]

Attack flow



Attack flow

- Acquire the target device
- Implant the sinffer
- Make sure the user enters their password
- Acquire the device, again
- Extract secrets from implant EEPROM
- Post-processing (dump all passwords)

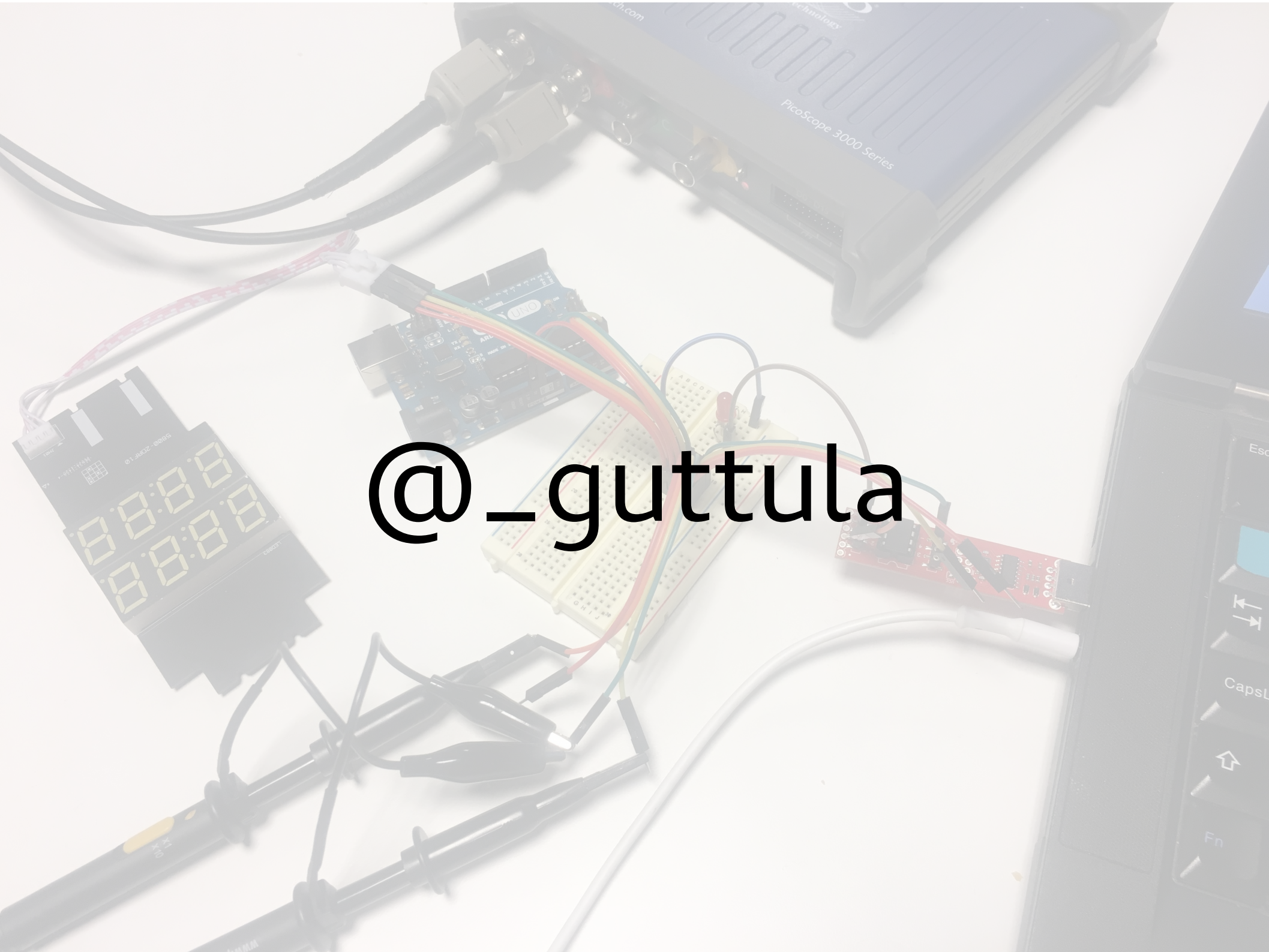
Mitigations

- Don't get your hardware "acquired"
- Make tampering visible
- Exclude this scenario from your list of valid attack scenarios and accept the risk

Pointers

<https://github.com/juhakivekas/two-wire-sniff>

<https://hackaday.io/project/18461-two-wire-sniff>



@_guttula