THOMAS MORE

Embedded Security

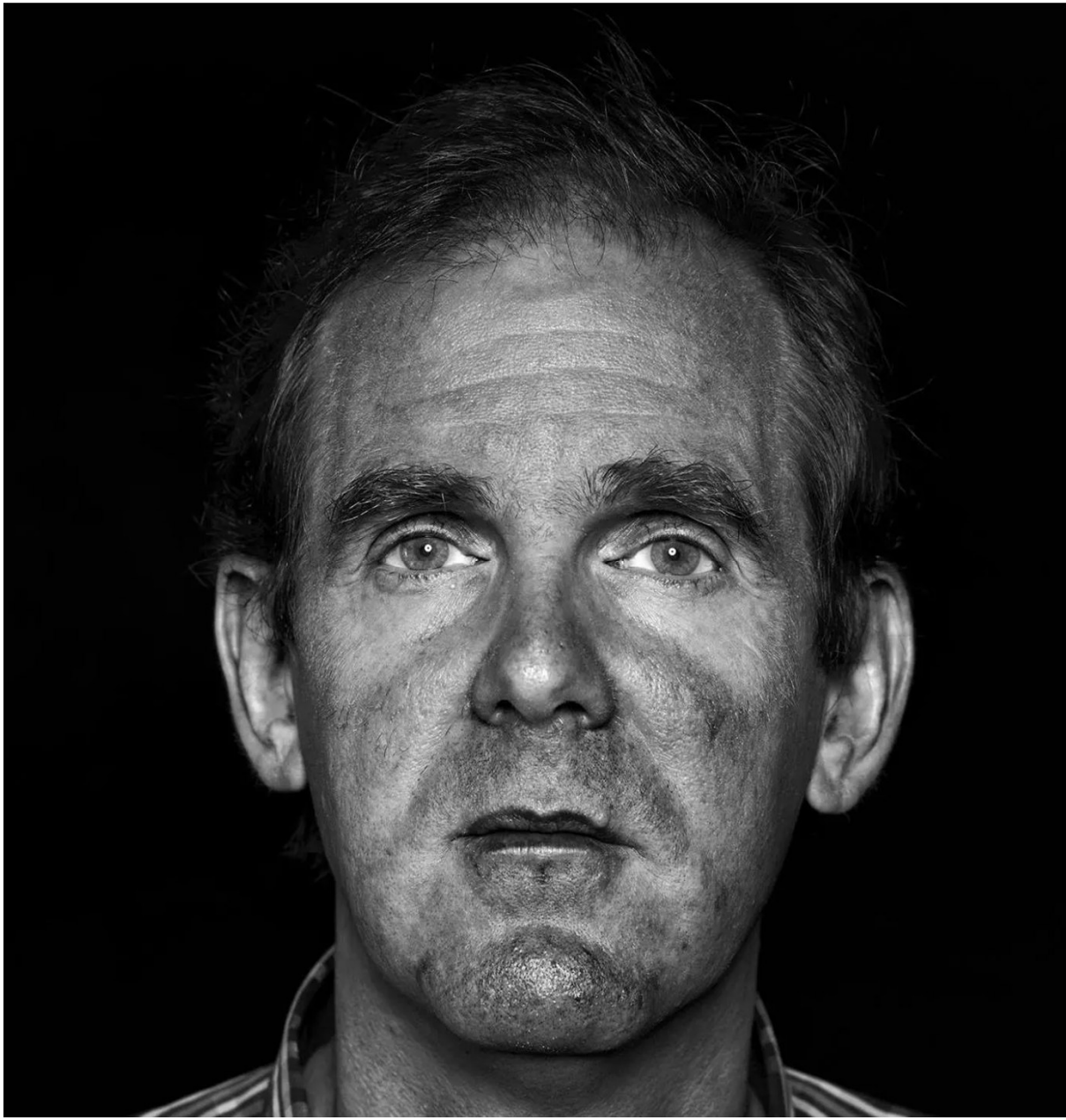
Hello!

Who am I?

- Maarten Van Lint – Thomas More, Belgium
- Expertise in electronic engineering (MSc)
- Coordinator workplace learning for IoT
- Teaching embedded systems / projects

Contact?

- Maarten.VanLint@thomasmore.be
- LinkedIn



Content

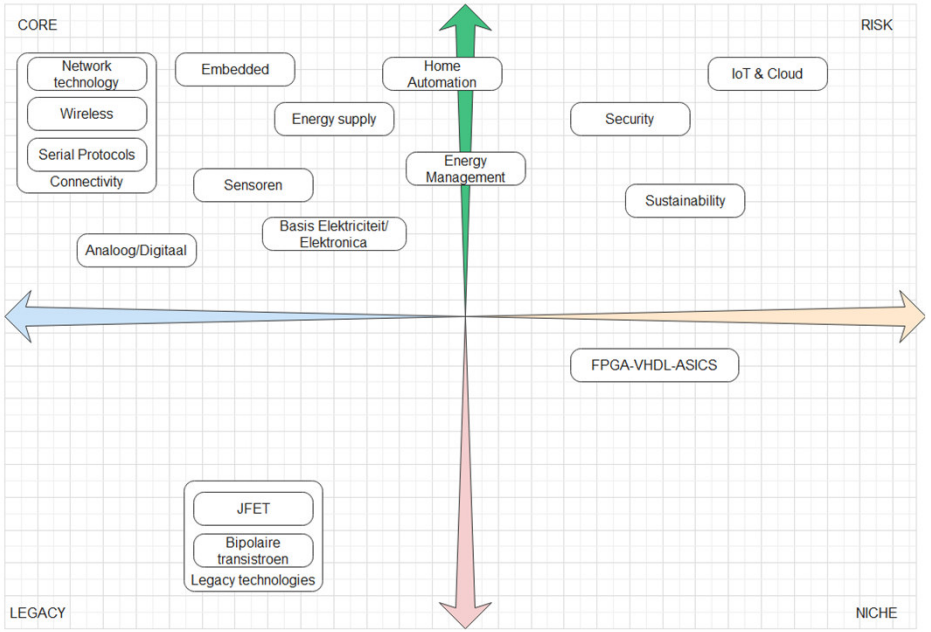
- Associate degree (short cycle) Internet of Things* and its approach
- Embedded security as part of the program
  - Approach
  - Content
  - Example: side channel attacks (power tracing)

Associate degree Internet of Things

- Name doesn't fit very well ⇨might change in (near) future
- Embedded systems oriented
- 2 year program
  - Very practical
  - Nevertheless: you need to know before being able to do
  - 3 semesters courses & projects
  - 1 semester internship (workplace learning)

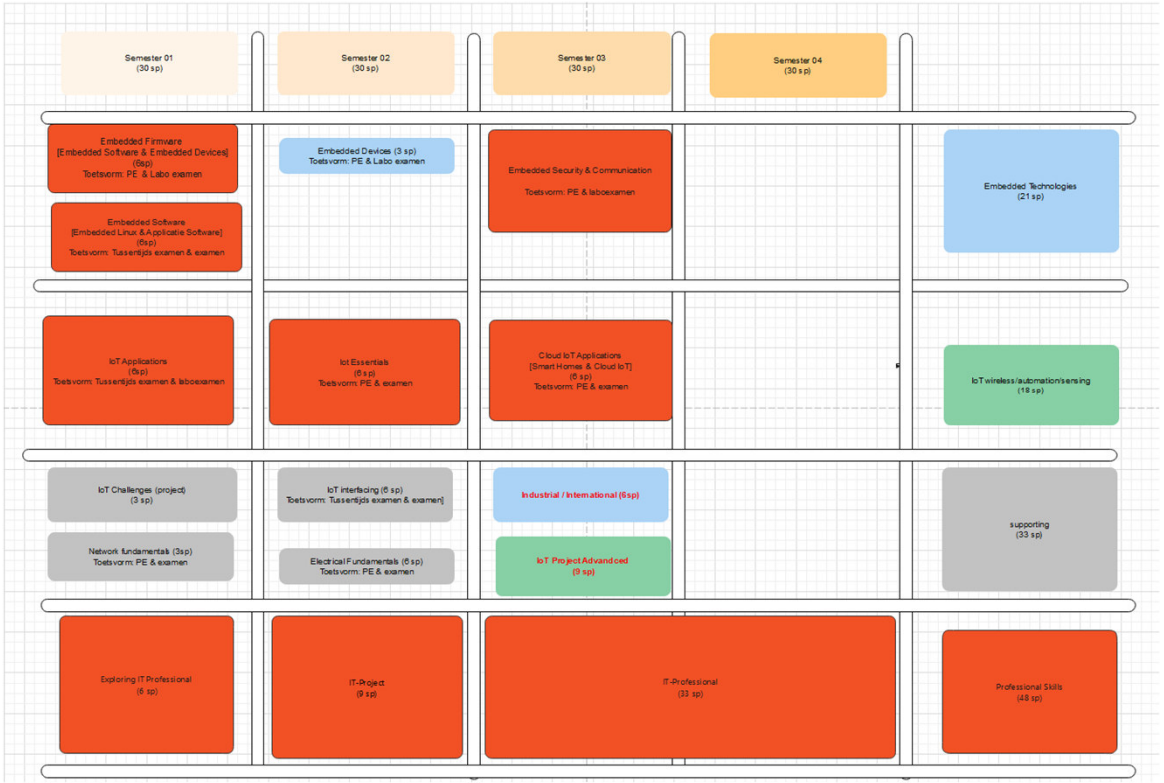
Embedded security as part of the program

- Yearly: 2 advisory committees
  - Alignement with industry
  - Prepearation:



Embedded security as part of the program

- Result: Embedded security = part of a course



Embedded security - aproach

- At start
  - A lot of
    - Theory
    - Examples
    - Only a single lab
  - Not very motivating ⇨ new approach needed

Embedded security - aproach

- Since academic year 2025 -2026
  - Aproach:
    - Know how your devices is attacked ⇨ take precautions
    - More practical
      - Students practically
        - Implement counter measures
        - Hack embedded devices
          - Think about counter measures (and try to hack it again)

Embedded security - content

- Only 7 courses of 4,5 hours (= 31,5 hours)
- Not completed yet
  - Course starts at second part of this semester
- What should be in?
  - Introduction on methods (theory)
  - Explanation of certificates (theory)
  - Implementation of secure MQTT (lab)
  - Side channel attacks (labs)
    - Password recovery with power traces
    - AES key recovery with power traces
  - Software Defined Radio & hacking (labs)
  - Regulations (desk research?)

Embedded security - demo

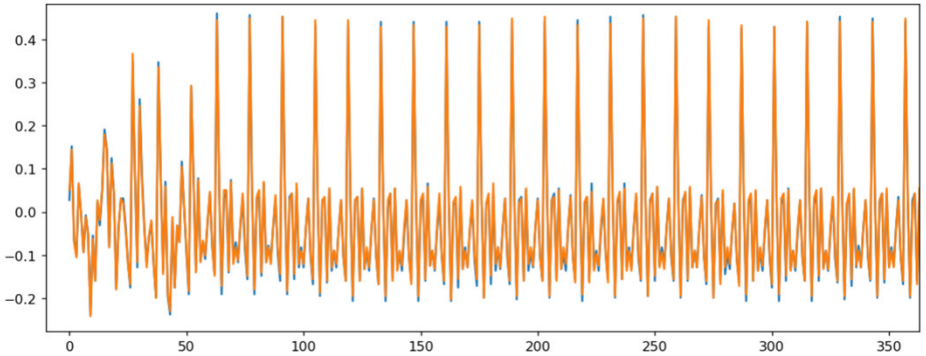
- Side channel attacks with Chipwhisperer from NewAE

What is it about?

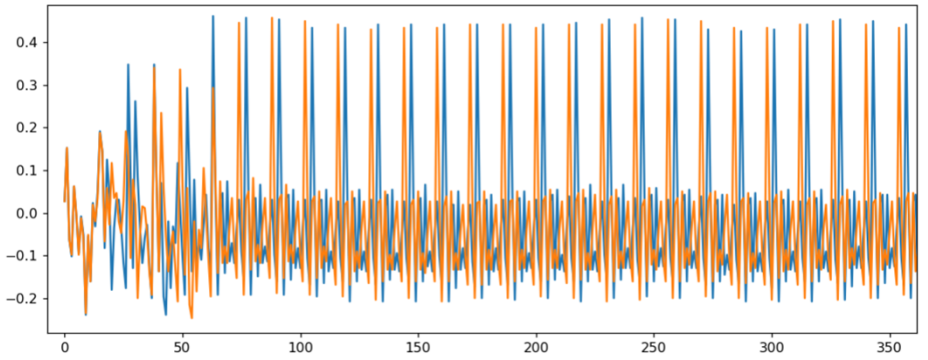
- Microcontrollers consume power like other devices
  - Depends processing load

Power analysis and passwords

- The trick



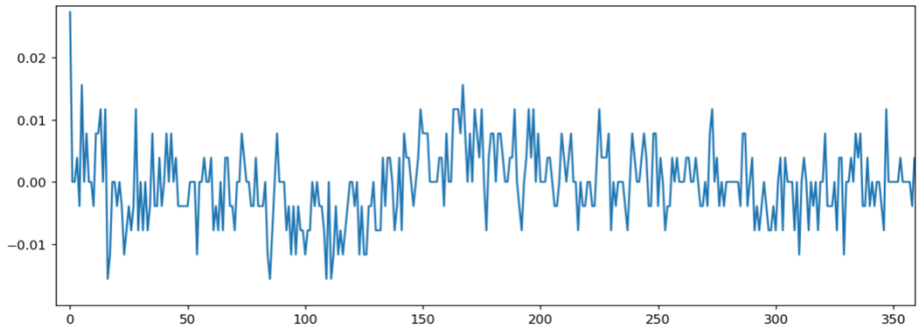
Power traces of two false characters



Power traces of correct character and a false character

Power analysis and passwords

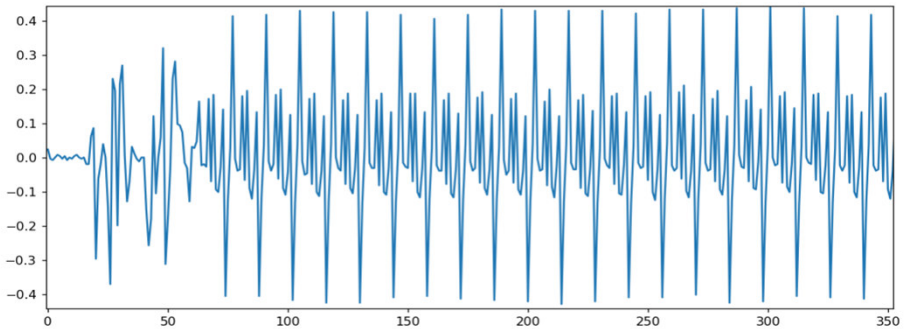
- The trick



Difference of false character with false reference

```
import numpy as np
diff = np.sum(np.abs(trace_testx-trace_test))
print (diff)
```

```
16.3046875
```



Difference of correct character with false reference

```
import numpy as np
diff = np.sum(np.abs(trace_testx-trace_test))
print (diff)
```

```
410.69140625
```

Power analysis and passwords

- It seems....
  - Power traces differ in password check when input is correct or wrong
  - Powertraces of an incorrect characters are similar
  - Powertrace of correct character is very different
- The trick
  - Make a powertrace of a character which is surely incorrect (eg NULL, not the best)
  - Compare the average (sum of absolute sample values) of powertrace with all possible characters until you get a huge difference (the power difference)

Power analysis and passwords

```
['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '0', '1', '2', '3',
'4', '5', '6', '7', '8', '9']
What is de maximum characters for the password?  1000
Guessing character 1
b
Guessing character 2
ba
Guessing character 3
ban
Guessing character 4
bana
Guessing character 5
banan
Guessing character 6
banana
Guessing character 7
bananas
Guessing character 8
bananas4
Guessing character 9
bananas4f
Guessing character 10
bananas4fr
Guessing character 11
bananas4fre
Guessing character 12
bananas4free
Guessing character 13
no character found; this means the password has 12 characters.
Finnished recovering; your password is: bananas4free
```

Thanks!

Maarten.VanLint@thomasmore.be