Side-channel based intrusion detection for industrial control systems

“I have no idea what this device is doing, but at least it’s still doing the same thing.”

CRITIS 2017, October 9th, 2017

CRITIS 2017

Pol Van Aubel

iCIS | Digital Security
Radboud University

Authors

Joint work:

Pol Van Aubel
pol.vanaubel@cs.ru.nl

Radboud University
iCIS|Digital Security

Kostas Papagiannopoulos
k.papagiannopoulos@cs.ru.nl

Radboud University
iCIS|Digital Security

Łukasz Chmielewski
chmielewski@riscure.com

Riscure BV

Christian Doerr
c.doerr@tudelft.nl

Delft University of Technology

Outline

Software behaviour verification

Side-channel analysis

Proposed system

Results

Future work, conclusions, and discussion

Outline

Software behaviour verification

Side-channel analysis

Proposed system

Results

Future work, conclusions, and discussion

The scenario

What if an attacker changes the software on the control systems?

- Natanz
- Ukraine
- . . .

The problem

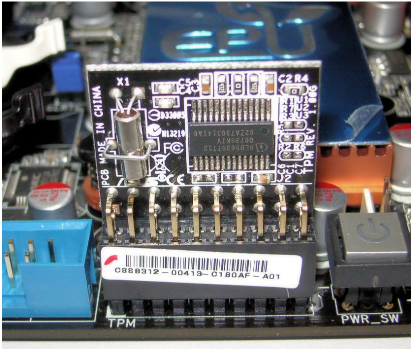
After a program is

- written
- tested
- deployed

how do we ensure that we are always running that program?

Prevent other software from running

Verify software signatures with a Trusted Platform Module.



Or similar solutions, requiring integration.

Detect when other software is running

- Network intrusion detection . . . and prevention?
- Host intrusion detection.

Requiring integration.

May be circumvented or worse.

What about the legacy?

Large number of deployed systems.

We need an option that can be used

- without software modifications,
- without hardware modifications,
- at most superficial hardware additions.

There are no silver bullets.

Side-channel based intrusion detection

We propose a system to detect software compromise of embedded industrial control systems by using the electromagnetic side-channel emissions of the underlying hardware.

Outline

Software behaviour verification

Side-channel analysis

Proposed system

Results

Future work, conclusions, and discussion

Side-channels

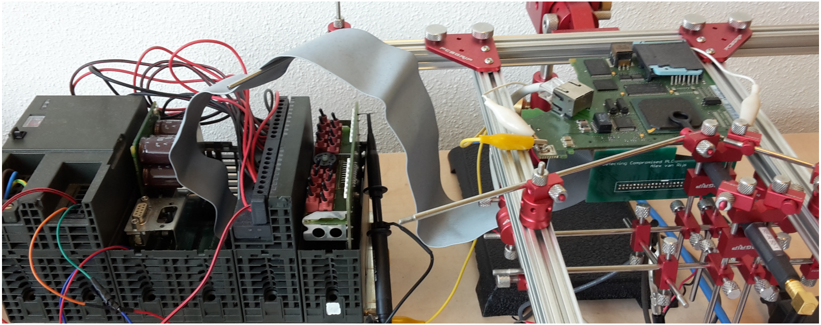
What is a side-channel?

Non-functional transmission of information about the state of a system.

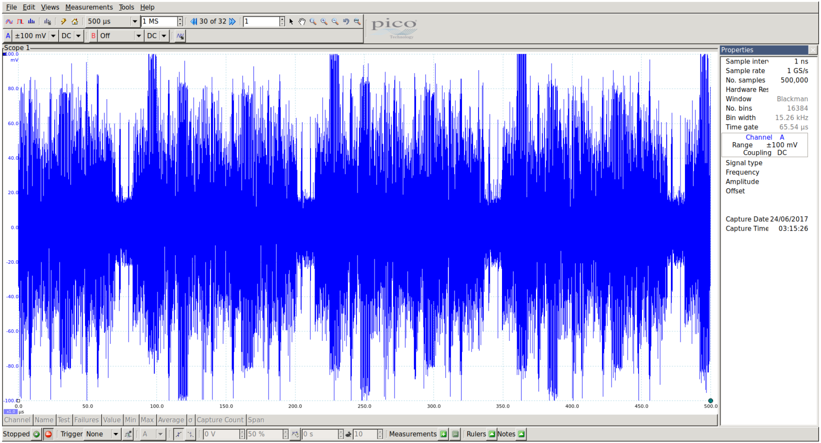
- Execution time
- Processor temperature
- Power consumption
- Coil whine
- WiFi power levels
- Electromagnetic radiation

Mostly used for breaking cryptography / security / privacy.

How to capture EM-radiation?



What does it look like?



Sample inter 1 ns
Sample rate 1 GS/s
No. samples 500,000
Hardware Res
Window Blackman
No. bins 16384
Bin width 15.26 kHz
Time gate 65.54 µs

Channel A
Range ±100 mV
Coupling DC

Signal type
Frequency
Amplitude
Offset

Capture Date 24/06/2017
Capture Time 03:15:26

PLCs 101

Dedicated industrial computers that are built for

- stability,
- robustness,
- real-time characteristics,
- and huge numbers of I/O arrangements.

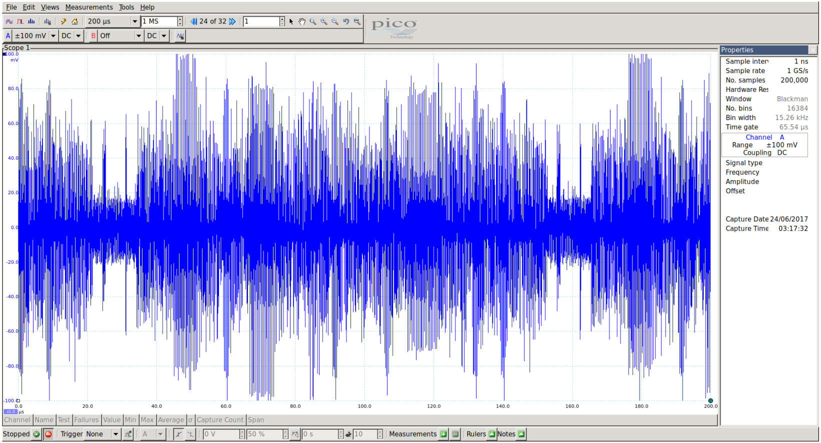
PLCs 101

Operate on a “scan cycle”:

1. read all inputs into memory,
2. execute the user program,
3. do error handling and other stuff,
4. drive all outputs from memory.

over and over again.

What does it look like?



Sample inter 1 ns
Sample rate 1 GS/s
No. samples 200,000
Hardware Res
Window Blackman
No. bins 16384
Bin width 15.26 kHz
Time gate 65.54 µs

Channel A
Range ±100 mV
Coupling DC

Signal type
Frequency
Amplitude
Offset

Capture Date 24/06/2017
Capture Time 03:17:32

Outline

Software behaviour verification

Side-channel analysis

Proposed system

Results

Future work, conclusions, and discussion

Attacker model

Attacker can upload new software to the PLC to replace or modify the existing user program.

Attacker cannot control the PLC operating system.

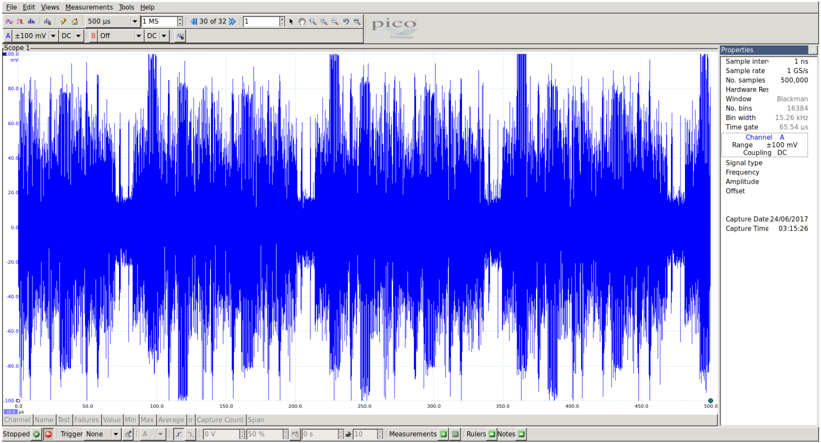
Two-layered intrusion detection

1. Timing layer: check program runtime.
2. EM layer: compare program EM trace to baseline.

Timing side-channel layer

- Trivially detects large alterations.
- Determining runtime?
  - EM-analysis
  - OS-emitted signal

Determine runtime through EM-analysis



Sample inter	1 ns
Sample rate	1 GS/s
No. samples	500,000
Hardware Res	
Window	Blackman
No. bins	16384
Bin width	15.26 kHz
Time gate	65.54 µs
Channel	A
Range	±100 mV
Coupling	DC
Signal type	
Frequency	
Amplitude	
Offset	
Capture Date	24/06/2017
Capture Time	03:15:26

EM side-channel layer

Distinguish between programs with minor modifications

- in program logic (instructions).
- in comparison constants (values).

Outline

Software behaviour verification

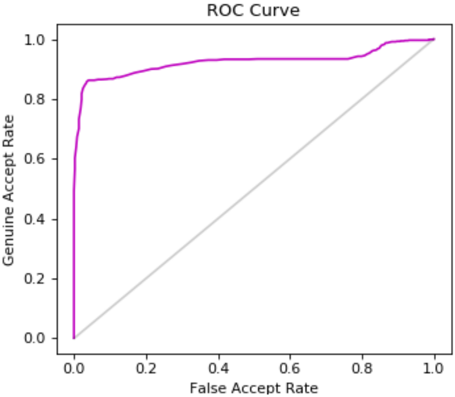
Side-channel analysis

Proposed system

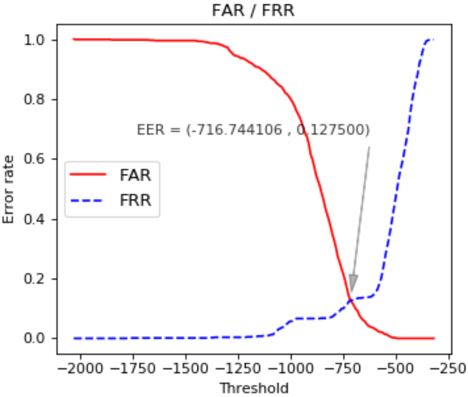
Results

Future work, conclusions, and discussion

Best results – comparison constant

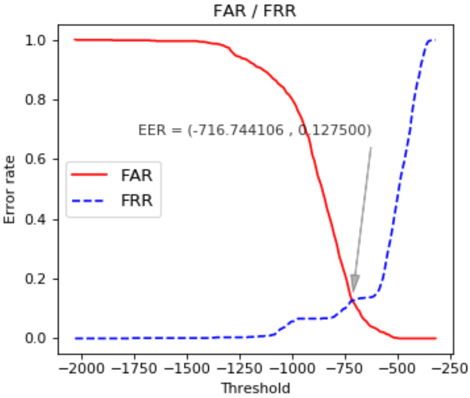


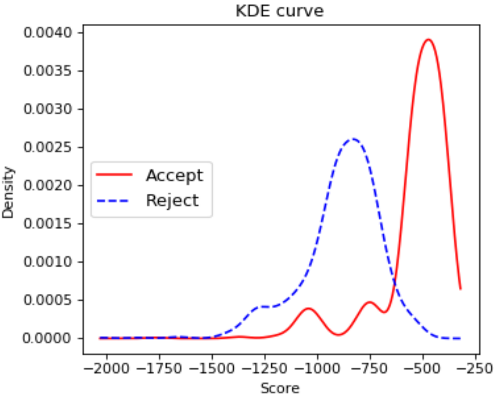
ROC Curve



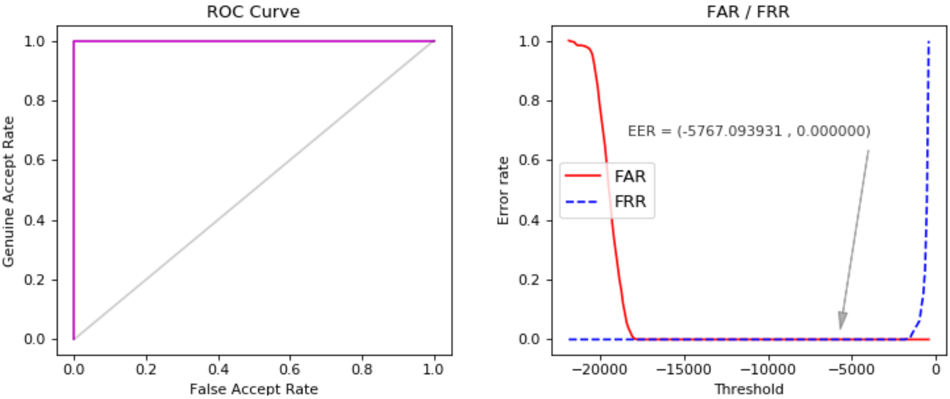
FAR / FRR

Best results – comparison constant



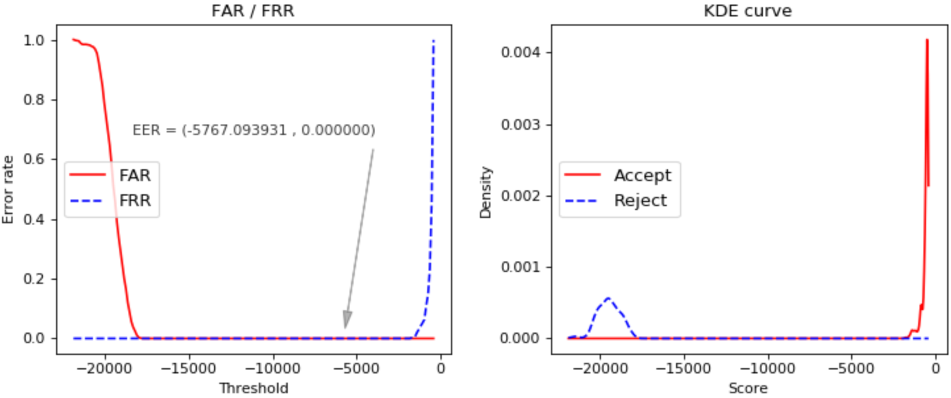


Best results – program logic



EER = (-5767.093931 , 0.000000)

Best results – program logic



Outline

Software behaviour verification

Side-channel analysis

Proposed system

Results

Future work, conclusions, and discussion

Future work

- Expand on classification techniques to improve recognition rates.
- Consider the PLC operating system.
- Analyse the impact of EM-noisy environments.

Main conclusions

- Our method is feasible.
- However, it does not come without a cost.
- Detects when attacker replaces user program.
- Software available at https://polvanaubel.com/research/em-ics/code/.

Pol Van Aubel

pol.vanaubel@cs.ru.nl

PGP key fingerprint:
5937 4550 F873 5C57 A778
BDE2 B563 848A 5F60 0EAE

Kostas Papagiannopoulos

k.papagiannopoulos@cs.ru.nl

Łukasz Chmielewski

chmielewski@riscure.com

Christian Doerr

c.doerr@tudelft.nl

Paper 59
on the conf. USB