PB173 Domain specific development: side-channel analysis

Course organization

Łukasz Chmielewski (chmiel@fi.muni.cz),
Milan Šorf (500362@mail.muni.cz)

Consultation: in A406 on Fridays 9:30-11:00
(please email Łukasz before coming)

CROCS

Centre for Research on
Cryptography and Security

Course info

- First seminar of this type
- Practical focus (hands-on):
  1. Learning what side-channel analysis is
  2. Working with ready tools and libraries
  3. Implementing your own tooling/scripts
- Style of seminars is usually:
  - small intro at the beginning of every seminar with materials and tasks
  - individual (Step 1-2)/team work (Step 3)
- Discussion:
  - ask (me) when stuck (within the seminar),
  - IS discussion group if everybody might be interested

Course info cont’d

- Today is different, a lecture called:
  “Introduction to side-channel analysis: Trust, trusted element, usage scenarios, side-channel attacks “

- Demo charging station attack.

- Look at one trace set (if we do not manage to do it today – look at that at home and give me an answer on the next seminar)

- We have to start somewhere

Seminars overview
(13 weeks / 11 seminars)

- First 1-4 seminars: “Introduction to side-channel analysis”:
  - Lecture
  - Demos
  - Inspecting Traces
  - Exercises with ChipWhisperer Acquisition
  - Implementing CPA and DPA
  - Inspecting More Traces
- Seminar 5 – choosing the project topic and the team
  - Which kind of side-channel tool you would like to implement?
- Seminar 5/6-12 – implementing tooling
- Seminars 11 and 12 are missing due to national holidays
  - we can schedule extra dates for consultations
- Seminar 13 – presentations / utilization

Project

- Second part of the semester
  - Teams of 3 or 2 people.
- Implement using existing tools or design your own (+10 points)
  - Present your tool script and its usefulness (+2 points)
- For your code:
  - Github repository + individual commits
- Trace sets:
  - From me or
  - Find on your own
- Possible Topics:
  - Trace Alignment
  - Manual Analysis of Traces: displaying, zooming, etc.
  - Implementing Classical Attacks: Differential/Correlation Power Analysis, Mutual Information Analysis, etc.
  - Filtering techniques: bandpass filters, etc.
  - Compression Techniques: windowed compression, frequency-based compression
  - More difficult, dimension reductions: Linear Regression and Principal Component Analysis
  - …

Colloquium

- To get the colloquium
  - You must be present at seminars (2 absences OK)
  - You must be active at seminars (+2 points given by me at the end)
  - You must submit and get:
    - 50%: 7 points in total

      (projects + presentation + activity = 14 points)

People

- Łukasz Chmielewski (CRoCS@FI MU)
  - Office hours (consultation): Friday 9:30-11:00, A406
  - Contact me first ↓

  chmiel@fi.muni.cz

  https://keybase.io/grasshoppper

  @chmiel:fi.muni.cz
- Milan Šorf (CRoCS@FI MU)
  - Office hours (consultation): Friday 16:00-18:00, A403
  - Contact me first ↓

  xsorf@fi.muni.cz,

  https://keybase.io/milan_s

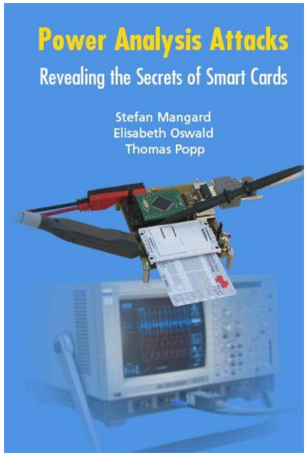
  @xsorf:fi.muni.cz

Homework

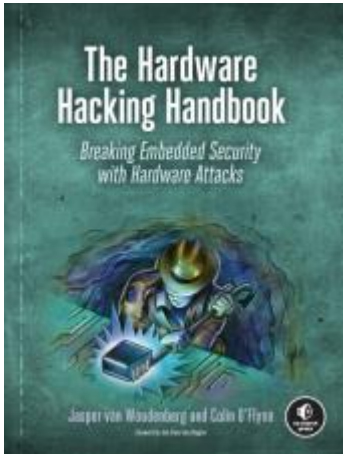
- TODOs before the next seminar:
  - Install ChipWhisperer: https://chipwhisperer.readthedocs.io/en/latest/linux-install.html
  - Read the website in general. I am using CW in a linux VM under Windows but do as you prefer ☺
- Watch
  - “PV204 Security technologies: Trust, trusted element, usage scenarios, side-channel attacks” by P. Svenda
  - See: pv204video2020.zip and PV204_03_SideChannelAttacks_2020.pdf in IS

Reading

- For interested people
- Side-Channel Analysis – blue book:
  - http://dpabook.iaik.tugraz.at/
  - The books is available at the uni.
  - Look online



- The Hardware Hacking Handbook:
  - https://nostarch.com/hardwarehacking
  - I have an epub version.


The Hardware Hacking Handbook
Breaking Embedded Security with Hardware Attacks
Jasper van Woudenberg and Colin O'Flynn

Questions