

SmartCard Lab



Starting Situation

What you get:

- Reference implementation of a PayTV card
- PCs with card readers and programming environment for microcontrollers
- -> Oscilloscope and MatLab interface
- -> Streaming server for PayTV
- -> Streaming software as Python script
- Relevant standards and brief description of the lab with references to further literature
- -> GitLab project for version

U

First introduction

Answers the following questions: What is the goal?

- -> Improve the security of a PayTV card.
- What is needed to acheive it?
- -> Understand the attack
- -> Perform the attack
- -> Implement a SmartCard on a microcontroller
- -> Implement countermeasures

Final hand-in criterion: Tradeoff evaluation between number of traces needed to successfully

attack the card and the cost of

Introduction to DPA

Introduction to the differential power analysis:

How does the AES algorithm work?

How is the AES attacked and why?

How can the attack be conducted?

Optional: Presentation of an attack in the lab on the reference implementation

Create project plan

Present project goals

Pre-Lab Assignment: Python and AVR tutorials

- -> Perform DPA
- -> Extract kev
- -> Documentation

III A



Practical tasks - Team A

- -> Implement card on microcontroller
 - + Documentation
- -> Build test environment
- -> Implement T=0 protocol III B

25.04.2019 13:15 - 14:45

02.05.2019 13:15 - 14:45

Integration phase

Extracted key is used in own implementation to build a clone card

The clone card must perform in the same way as the reference card. This defines the allowed timings etc.

IV

Milestone

Presentation of some results on a fixed date (midterm)

Students will get information about different countermeasures, select some of them for the final version and present the current implementation.



Practical tasks - Team B

- -> Perform DPA on clone card
- -> Determine the number of traces

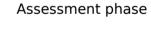
neccessary to get the key
VI B



Practical tasks - Team A

- -> Implement countermeasures (Mask., Wait...)
- -> Documentation

VI A



Presentation by students:

- -> What is the benefit of taking countermeasures?
- -> What do they cost?
- -> Results of the work

student

Submission of documentation: -> Protocol of activities per

- -> Tasks worked on
- -> Interesting results
- -> As Wiki in GitLab (preferred)
 Oral examination

VII

11.07.2019 09:00 - 12:00 Oral exam: 18.07.2019 09:00 - 13:30

06.06.2019 12:30 - 15:30