

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
- -> TRAC server for documentation

0

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: Number of traces needed to successfully attack the card

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

April 20, 2015 - 11:30 - 13:00

Practical tasks - Team A

- -> Perform DPA
- -> Extract key
- -> Documentation

III A

Practical tasks - Team B

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

III B

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

April 13, 2015 - 11:30 - 13:00

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.



Pre-Lab Assignment:

Matab and AVR tutorials

Practical tasks - Team B

- -> Perform DPA on clone card
- -> Determine the number of traces neccessary to get the key

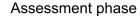
VI B



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

Submission of documentation:

- -> Protocol of activities per student
 - -> Tasks worked on
 - -> Interesting results
- -> As TRAC Wiki (preferred)

Oral examination

VII

July 14, 2015 - 09:00 - 12:00 July 21, 2015 - 09:00 - 12:00

June 16, 2015 - 09:00 - 12:00