Remote relay attack on RFID access control systems (Project 30)

8 feb 2013

Wouter van Dullink & Pieter Westein

Summary

- Research question
- RFID Background
- ISO 14443
- Relay attack landscape
- Demo
- Questions

Research question

- How can you perform a relay-attack, using a network channel, between two NFC enabled devices?

RFID Background

- RFID is a technology that uses electromagnetic waves to identify object, animals or people in an unique manner.

RFID Basics

RFID Basics


tag reader
traffic monitoring camera
E-ZPass tag
traffic gate
5 MPH
REDUCE SPEED
PASS
The E-ZPass Process
©2001 HowStuffWorks
traffic information display

RFID Basics


Inlay with integrated contactless chip
Passport cover
SPECIMEN
ELECTRONIC PASSPORT

RFID Basics

RFID Background

	LF	HF	UHF
Freq. Range	125 - 134KHz	13.56 MHz	866 - 915MHz
Read Range	10 CM	1M	2-7 M
Coupling	Magnetic	Magnetic	Electro magnetic
Existing standards	11784/85, 14223	18000-3.1, 15693,14443	EPC C0, C1, C1G2, 18000-6

ISO 14443

- Split into 4 parts
  - Physical Characteristics
  - Modulation Techniques
  - Initialization Protocol
  - Transmission Protocol (optional)

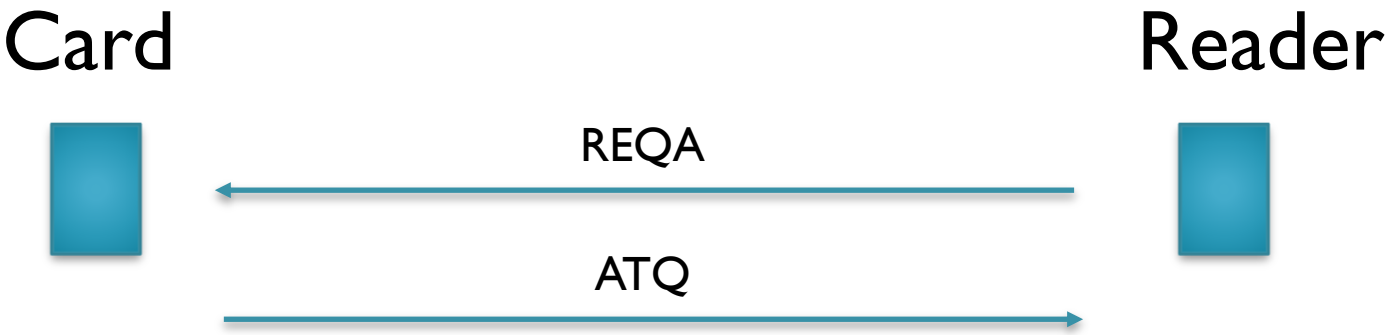
Initialization

Card

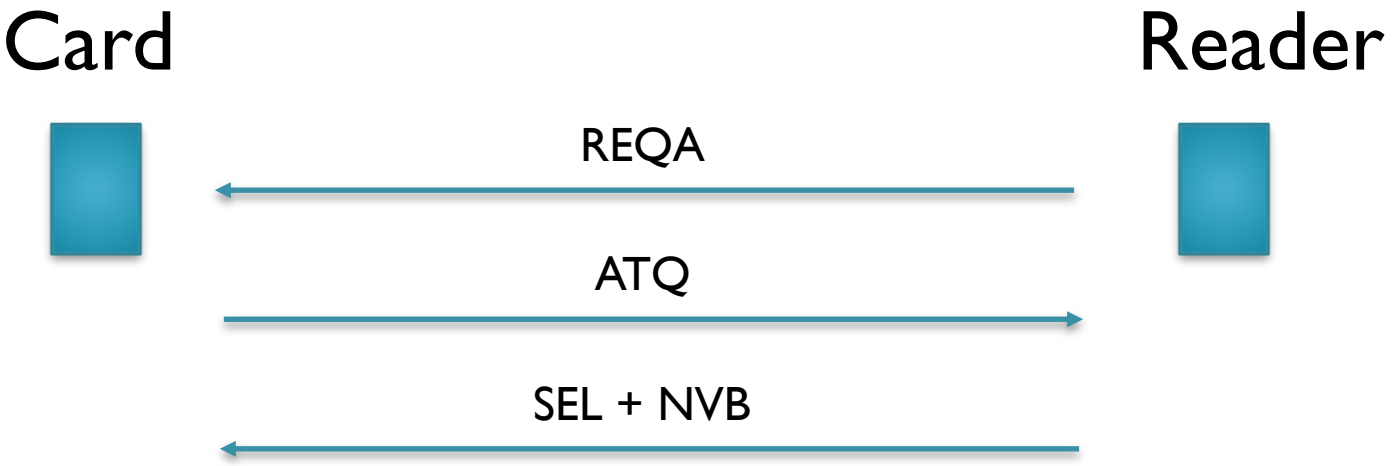
Reader

Initialization

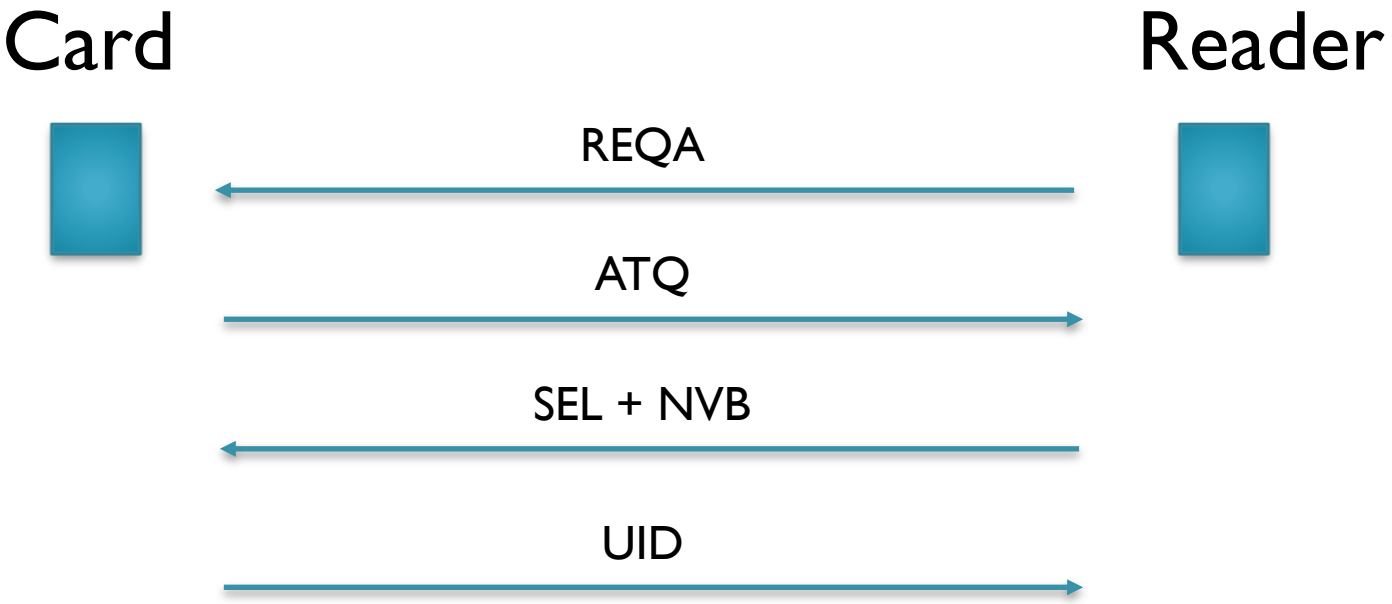
Initialization



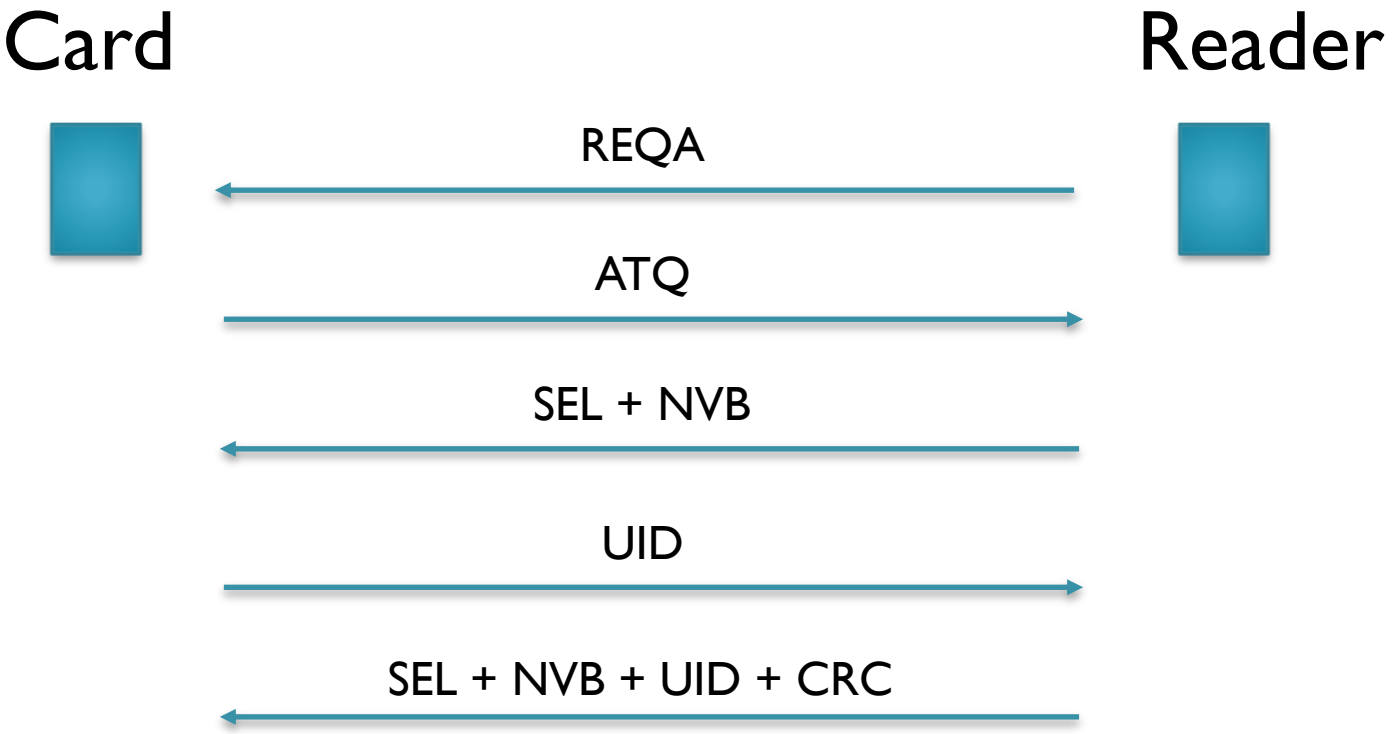
Initialization



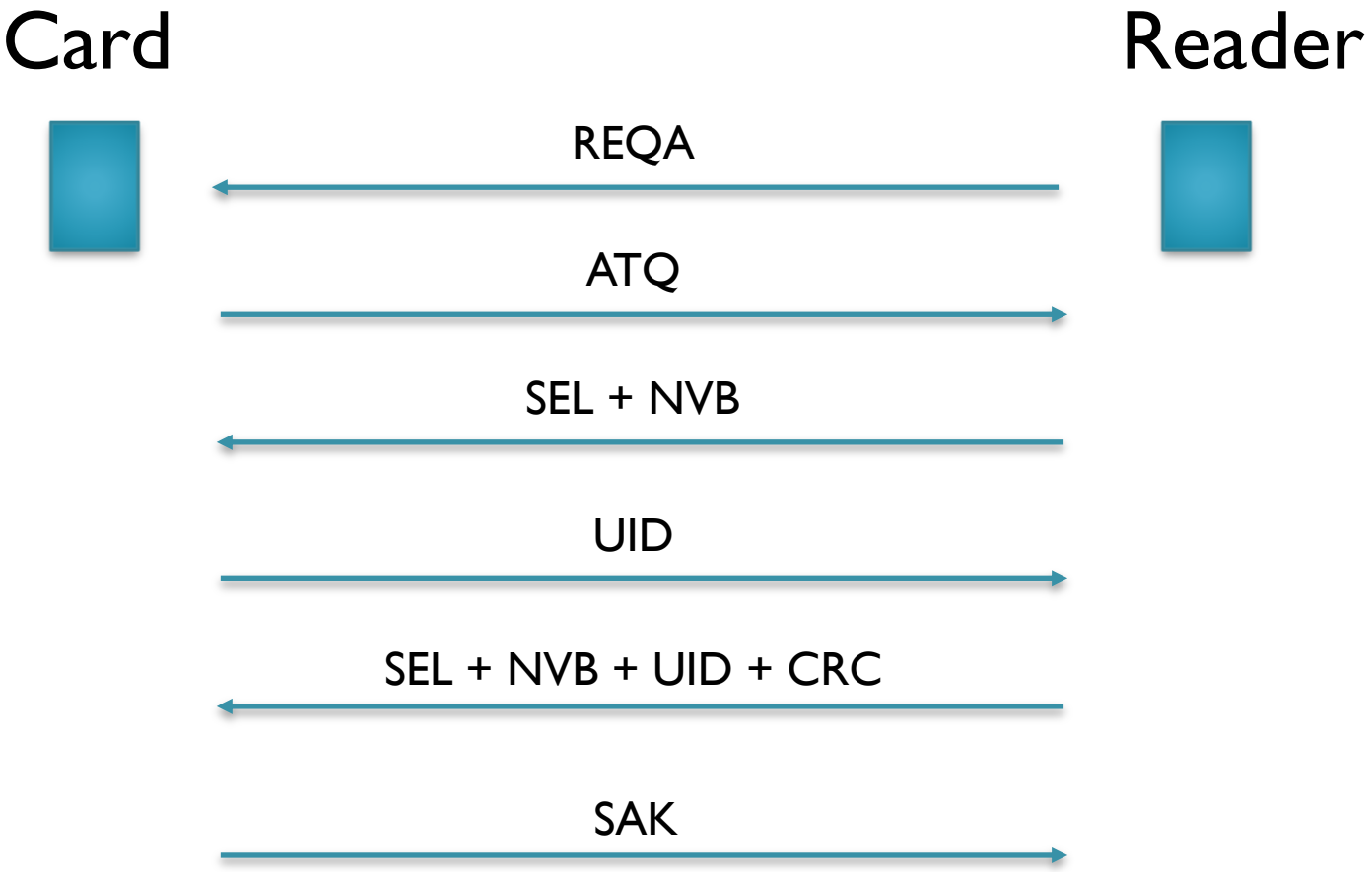
Initialization



Initialization



Initialization

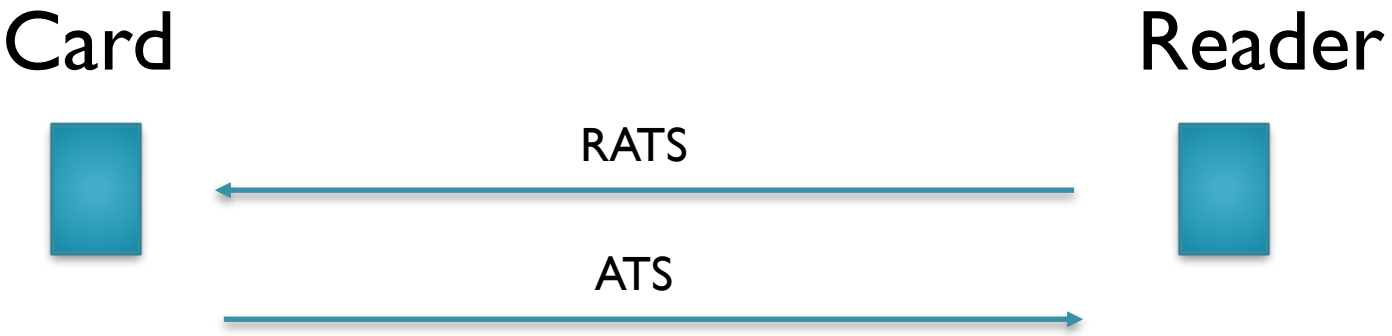


Transmission Protocol

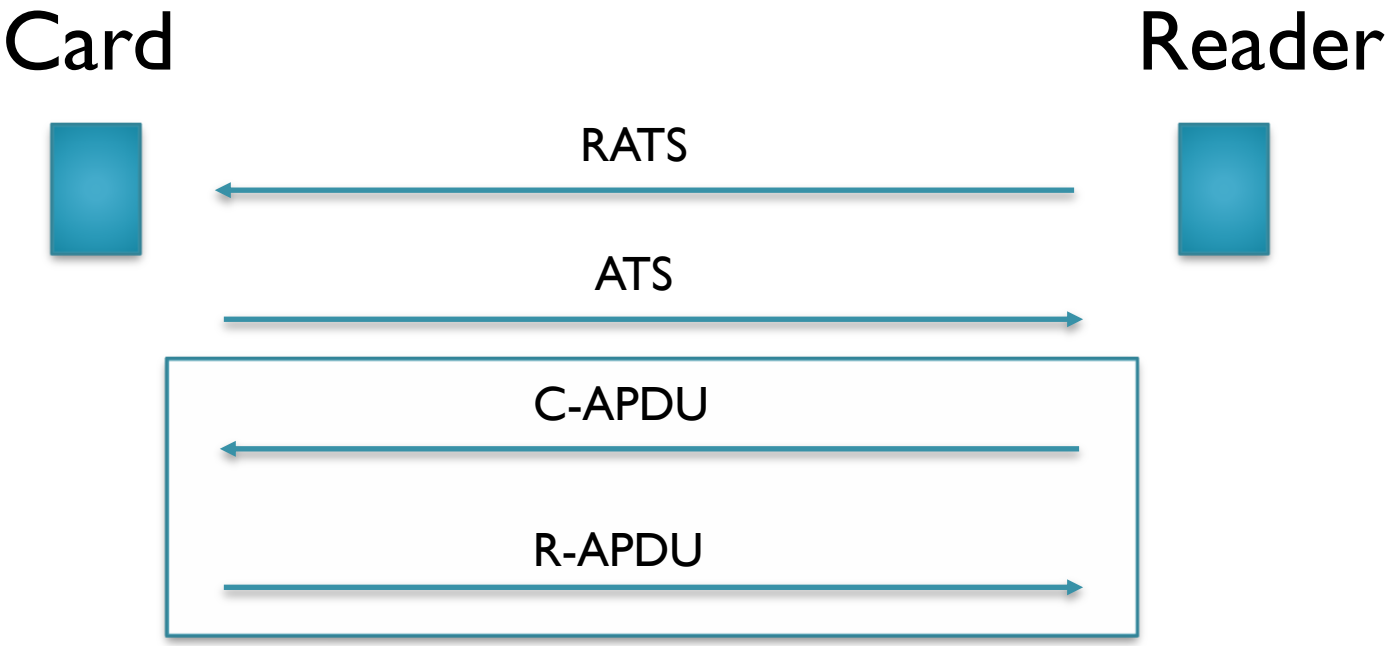
- Optional to choose
  - Also other protocols available
- Timing values
  - Frame Waiting Time
  - Waiting Time Extension

Transmission

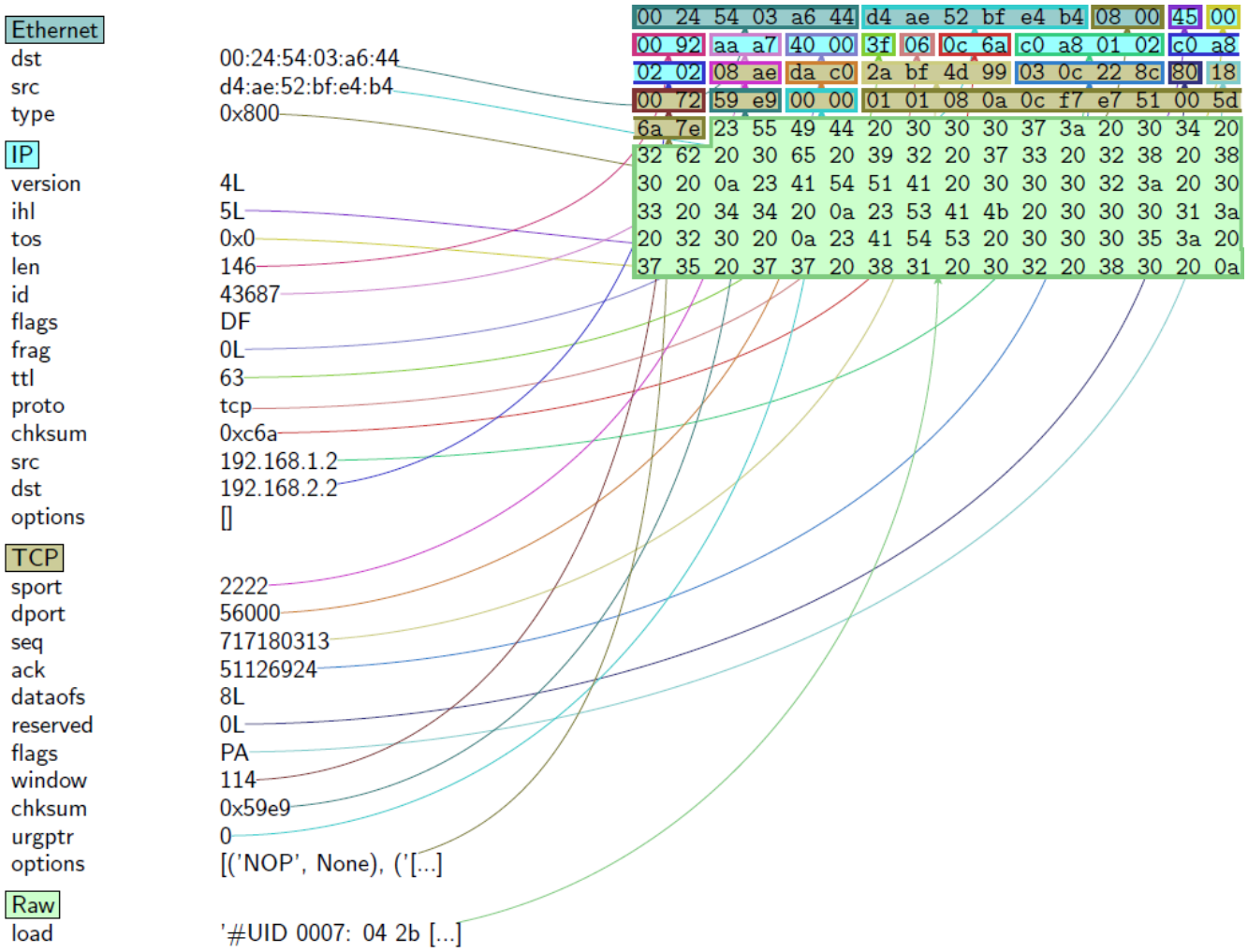
Transmission



Transmission



ATS Packet


Ethernet
dst 00:24:54:03:a6:44
src d4:ae:52:bf:e4:b4
type 0x800
IP
version 4L
ihl 5L
tos 0x0
len 146
id 43687
flags DF
frag 0L
ttl 63
proto tcp
chksum 0xc6a
src 192.168.1.2
dst 192.168.2.2
options []
TCP
sport 2222
dport 56000
seq 717180313
ack 51126924
dataofs 8L
reserved 0L
flags PA
window 114
chksum 0x59e9
urgptr 0
options [('NOP', None), ('[...]
Raw
load '#UID 0007: 04 2b [...]
00 24 54 03 a6 44 d4 ae 52 bf e4 b4 08 00 45 00
00 92 aa a7 40 00 3f 06 0c 6a c0 a8 01 02 c0 a8
02 02 08 ae da c0 2a bf 4d 99 03 0c 22 8c 80 18
00 72 59 e9 00 00 01 01 08 0a 0c f7 e7 51 00 5d
6a 7e 23 55 49 44 20 30 30 30 37 3a 20 30 34 20
32 62 20 30 65 20 39 32 20 37 33 20 32 38 20 38
30 20 0a 23 41 54 51 41 20 30 30 30 32 3a 20 30
33 20 34 34 20 0a 23 53 41 4b 20 30 30 30 31 3a
20 32 30 20 0a 23 41 54 53 20 30 30 30 35 3a 20
37 35 20 37 37 20 38 31 20 30 32 20 38 30 20 0a

ATS Packet - Details

23 55 49 44 20 30 30 30 37
3a 20 30 34 20 32 62 20 30
65 20 39 32 20 37 33 20 32
38 20 38 30 20 0a 23 41 54
51 41 20 30 30 30 32 3a 20
30 33 20 34 34 20 0a 23 53
41 4b 20 30 30 30 31 3a 20
32 30 20 0a 23 41 54 53 20
30 30 30 35 3a 20 37 35 20
37 37 20 38 31 20 30 32 20
38 30 20 0a

ATS Packet - Details

23 55 49 44 20 30 30 30 37
3a 20 30 34 20 32 62 20 30
65 20 39 32 20 37 33 20 32
38 20 38 30 20 0a 23 41 54
51 41 20 30 30 30 32 3a 20
30 33 20 34 34 20 0a 23 53
41 4b 20 30 30 30 31 3a 20
32 30 20 0a 23 41 54 53 20
30 30 30 35 3a 20 37 35 20
37 37 20 38 31 20 30 32 20
38 30 20 0a

#UID 0007: 04 2b 0e 92 73 28 80

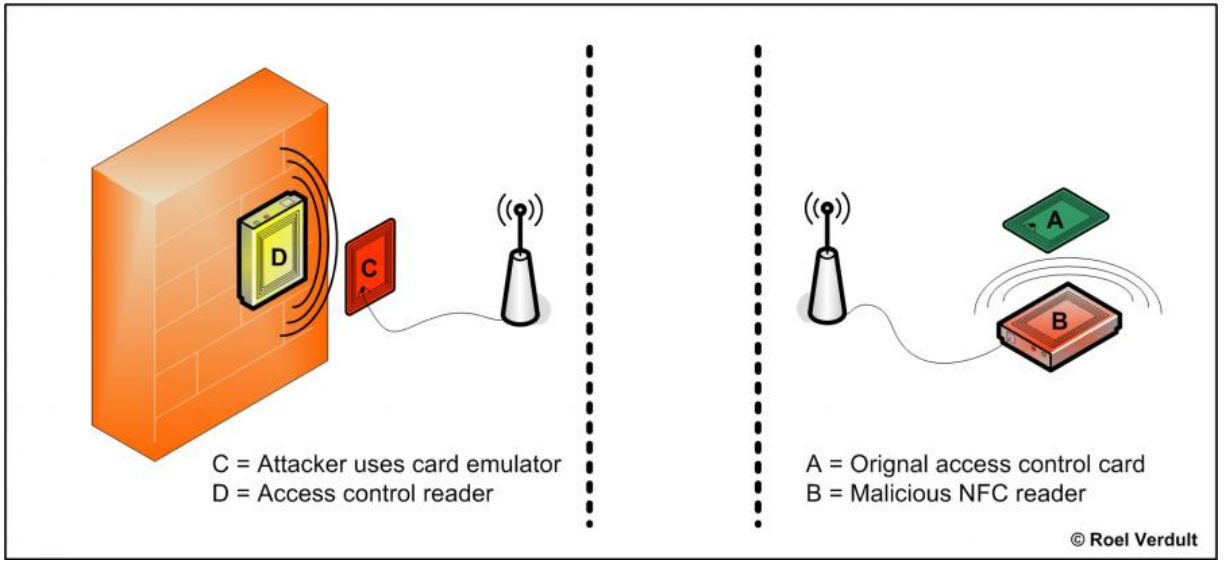
#ATQA 0002: 03 44

#SAK 0001: 20

#ATS 0005: 75 77 81 02 80

Relay attack landscape

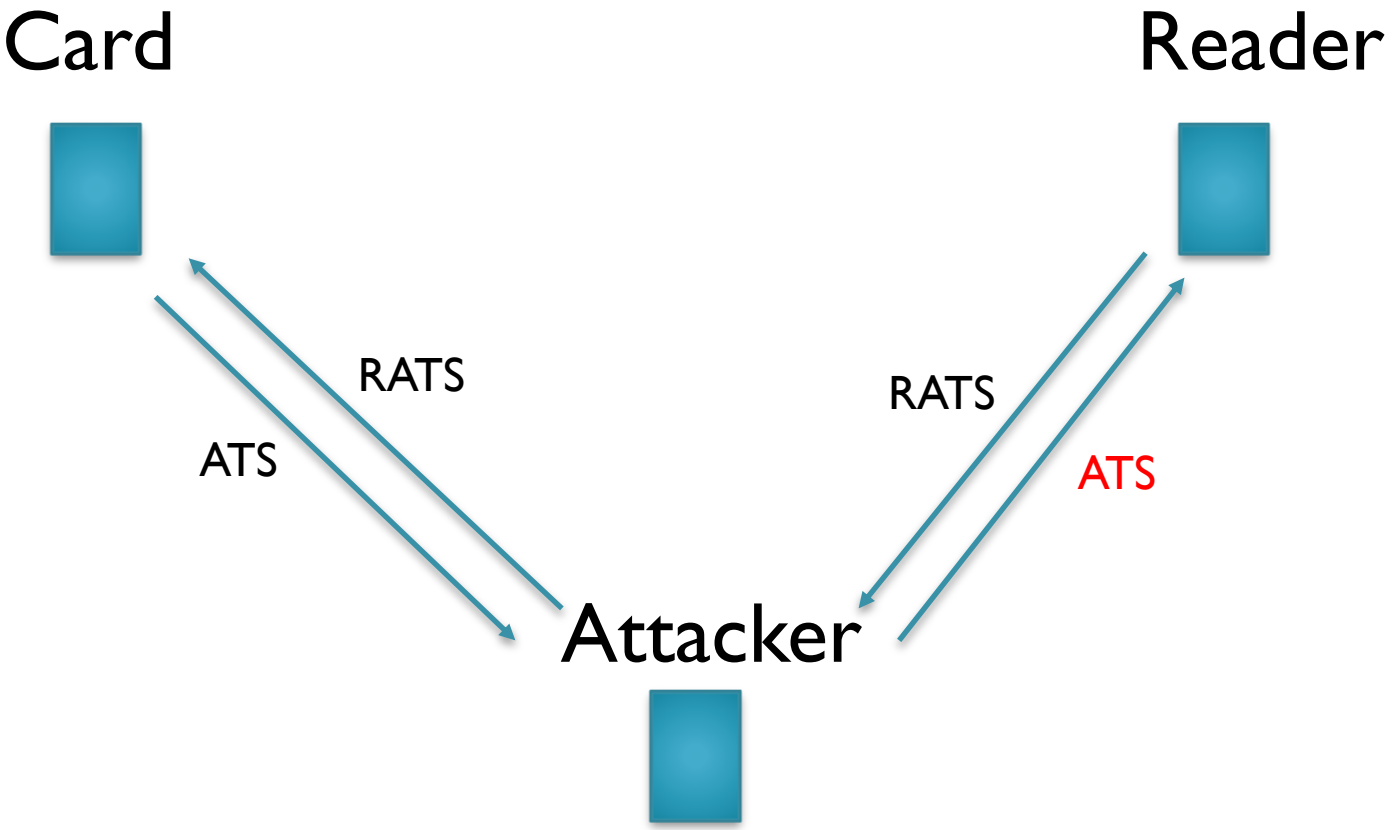
- Timing issues
- Relation with the standard



FWT attack

- Change FWT for each challenge-response
  - Modifying the FWI inside the ATS
  - Man in the Middle setup

Attack setup



1. Queue original ATS
2. Modify the FWI
3. Send the modified ATS

Demo

Conclusion

- Relay attack is possible, if the system supports ISO 14443-4.
- FWT is changeable by modifying the FWI
- Hardware dependent

Questions?

References

- UvA Logo: http://www.uva.nl/en/about-the-uva/uva-profile/corporate-identity/brand-identity-elements/logo/logo.html
- E-Z Proces: http://www.csb.uncw.edu/people/matthewskd/classes/mis213/chapters/08/images/8-4-1.png
- Passport: http://techfreep.com/images/epass1.jpg
- Acces control : http://img.tjskl.org.cn/nimg/ab/82/62ba10ee07b160de865a7e818a75-600x400-1/optical_turnstiles_with_access_control_system_single_and_bi_direction_control_for_station.jpg
- Rely attack : http://nfc-tools.org
- Demo Time : http://gopalshenoy.files.wordpress.com/2011/04/product_demos.jpg
- Questions : https://volunteer.colorado.edu/sites/default/files/question-marks.jpg