Relay attacks against the Mifare Desfire card

Experiments, results and limitations

IRISA
Embedded Security and Cryptography (EMSEC)

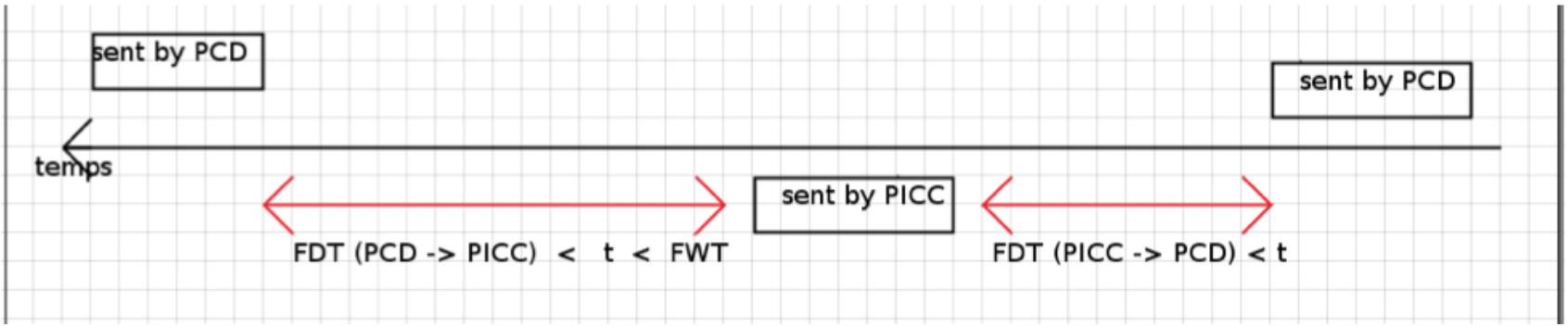
12/05/2015

Outline

ISO14443 standard : layers 3 and 4

Time constraints

- The protocol activation of ISO14443-4 A card ends with the transmission of the ATS response : 75 33 92 03 80 for example.
- This response contains valuable information used in the communication between the card and the reader.



Relevant time elements when doing relay attacks

- FWT : It defines the time within which a PICC shall start its response frame after the end of a PCD frame. It is calculated by the formula : $((256 * 16)/fc) * (2^{FWI})$
- S(WTX) : When the PICC needs more time than the defined FWT to process the received block it shall use an S(WTX) request for a waiting time extension.
- $FDT(PCD \rightarrow PICC)$: This time depends on the command, and it defines the minimum time between the last bit transmitted by the PCD and the first bit transmitted by the PICC.

Implementation
Time Constraints

- Response time : It defines the time between the last bit of the command and the first bit of the corresponding response received by the PCD. It is equal to $FDT(PCD \rightarrow PICC)$ when there are no other exchanges between the command and the response.
- Timeout : It defines the maximal value of the response time. When the reader embeds a PN53x chip, the timeout is calculated by the formula :
$Timeout = FWT + 3 * (2^{FWI})etu$

ACR122

- $528ms \leq Timeout \leq 778ms$

Timeout = 5s, Delay = 5s, Response time = 5.028s

Start Date	Sender	Frame	Byte...	Error	End Date	Duration	Timing	Protocol
7 474 487 640 ns	PCD_A	REQA	1 byte		7 474 582 040 ns	94 400 ns		14443
7 474 653 630 ns	PICC_A	ATQA	2 bytes		7 474 842 410 ns	188 780 ns	FDT PCD to PICC = 87.4 µs	14443
7 475 468 600 ns	PCD_A	ANTICOLLISION	2 bytes		7 475 666 840 ns	198 240 ns	FDT PICC to PCD = 640.6 µs	14443
7 475 738 390 ns	PICC_A	UID CLn	5 bytes		7 476 182 050 ns	443 660 ns	FDT PCD to PICC = 87.4 µs	14443
7 477 742 720 ns	PCD_A	SELECT	9 bytes		7 478 535 680 ns	792 960 ns	FDT PICC to PCD = 1.57 ms	14443
7 478 607 190 ns	PICC_A	SAK	3 bytes		7 478 880 930 ns	273 740 ns	FDT PCD to PICC = 87.4 µs	14443
7 479 478 800 ns	PCD_A	RATS	4 bytes		7 479 846 960 ns	368 160 ns	FDT PICC to PCD = 607.6 µs	14443
7 481 381 650 ns	PICC_A	ATS	8 bytes		7 482 080 170 ns	698 520 ns	FDT PCD to PICC = 1.56 ms	14443
7 499 829 040 ns	PCD_A	I(0)0	12 bytes		7 500 876 880 ns	1 047 840 ns	FDT PICC to PCD = 17.76 ms	14443
7 502 996 690 ns	PICC_A	S(WTX) Request	4 bytes		7 503 355 390 ns	358 700 ns	FDT PCD to PICC = 2.14 ms	14443
7 504 850 000 ns	PCD_A	S(WTX) Response	4 bytes		7 505 218 160 ns	368 160 ns	FDT PICC to PCD = 1.5 ms	14443
8 279 778 910 ns	PICC_A	S(WTX) Request	4 bytes		8 280 137 610 ns	358 700 ns	FDT PCD to PICC = 774.58 ms	14443
8 282 123 040 ns	PCD_A	S(WTX) Response	4 bytes		8 282 491 200 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
9 057 042 530 ns	PICC_A	S(WTX) Request	4 bytes		9 057 401 210 ns	358 680 ns	FDT PCD to PICC = 774.57 ms	14443
9 059 386 640 ns	PCD_A	S(WTX) Response	4 bytes		9 059 754 800 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
9 834 306 150 ns	PICC_A	S(WTX) Request	4 bytes		9 834 664 830 ns	358 680 ns	FDT PCD to PICC = 774.57 ms	14443
9 836 650 280 ns	PCD_A	S(WTX) Response	4 bytes		9 837 018 440 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
10 611 569 830 ns	PICC_A	S(WTX) Request	4 bytes		10 611 928 530 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
10 613 913 920 ns	PCD_A	S(WTX) Response	4 bytes		10 614 282 080 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
11 388 833 370 ns	PICC_A	S(WTX) Request	4 bytes		11 389 192 070 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
11 391 177 520 ns	PCD_A	S(WTX) Response	4 bytes		11 391 545 680 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
12 166 096 990 ns	PICC_A	S(WTX) Request	4 bytes		12 166 455 690 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
12 168 441 120 ns	PCD_A	S(WTX) Response	4 bytes		12 168 809 280 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
12 529 610 710 ns	PICC_A	I(0)0	5 bytes		12 530 054 350 ns	443 640 ns	FDT PCD to PICC = 360.82 ms	14443
12 540 478 400 ns	PCD_A	S(DESELECT)	3 bytes		12 540 761 600 ns	283 200 ns	FDT PICC to PCD = 10.43 ms	14443
12 541 267 350 ns	PICC_A	S(DESELECT)	3 bytes		12 541 541 090 ns	273 740 ns	FDT PCD to PICC = 526.3 µs	14443

SCL3711

- *Timeout* $\cong$ 158*ms*

Timeout = 3.28s, Delay =4 s, Response time > 3.099

Start Date	Sender	Frame	Byte...	Error	End Date	Duration	Timing	Protocol
5 062 483 520 ns	PCD_A	REQA	1 byte		5 062 577 920 ns	94 400 ns		14443
5 062 649 370 ns	PICC_A	ATQA	2 bytes		5 062 838 170 ns	188 800 ns	FDT PCD to PICC = 87.2 µs	14443
5 063 030 400 ns	PCD_A	ANTICOLLISION	2 bytes		5 063 228 640 ns	198 240 ns	FDT PICC to PCD = 206.4 µs	14443
5 063 300 410 ns	PICC_A	UID CLn	5 bytes		5 063 744 090 ns	443 680 ns	FDT PCD to PICC = 87.5 µs	14443
5 064 908 640 ns	PCD_A	SELECT	9 bytes		5 065 701 600 ns	792 960 ns	FDT PICC to PCD = 1.17 ms	14443
5 065 773 110 ns	PICC_A	SAK	3 bytes		5 066 046 850 ns	273 740 ns	FDT PCD to PICC = 87.3 µs	14443
5 066 729 920 ns	PCD_A	ANTICOLLISION	2 bytes		5 066 928 160 ns	198 240 ns	FDT PICC to PCD = 692.4 µs	14443
5 079 010 960 ns	PCD_A	ANTICOLLISION	2 bytes		5 079 209 200 ns	198 240 ns		14443
5 091 292 040 ns	PCD_A	ANTICOLLISION	2 bytes		5 091 490 280 ns	198 240 ns		14443
5 103 620 320 ns	PCD_A	REQA	1 byte		5 103 714 720 ns	94 400 ns		14443
5 103 786 190 ns	PICC_A	ATQA	2 bytes		5 103 974 990 ns	188 800 ns	FDT PCD to PICC = 87.2 µs	14443
5 104 167 240 ns	PCD_A	ANTICOLLISION	2 bytes		5 104 365 480 ns	198 240 ns	FDT PICC to PCD = 206.4 µs	14443
5 104 437 150 ns	PICC_A	UID CLn	5 bytes		5 104 880 830 ns	443 680 ns	FDT PCD to PICC = 87.4 µs	14443
5 106 045 440 ns	PCD_A	SELECT	9 bytes		5 106 838 400 ns	792 960 ns	FDT PICC to PCD = 1.17 ms	14443
5 106 909 990 ns	PICC_A	SAK	3 bytes		5 107 183 750 ns	273 760 ns	FDT PCD to PICC = 87.3 µs	14443
5 108 083 840 ns	PCD_A	RATS	4 bytes		5 108 452 000 ns	368 160 ns	FDT PICC to PCD = 909.6 µs	14443
5 109 977 310 ns	PICC_A	ATS	8 bytes		5 110 675 850 ns	698 540 ns	FDT PCD to PICC = 1.54 ms	14443
5 116 239 440 ns	PCD_A	I(0)0	12 bytes		5 117 287 280 ns	1 047 840 ns	FDT PICC to PCD = 5.58 ms	14443
5 119 416 730 ns	PICC_A	S(WTX) Request	4 bytes		5 119 775 450 ns	358 720 ns	FDT PCD to PICC = 2.15 ms	14443
5 120 175 240 ns	PCD_A	S(WTX) Response	4 bytes		5 120 543 400 ns	368 160 ns	FDT PICC to PCD = 409.4 µs	14443
5 895 209 690 ns	PICC_A	S(WTX) Request	4 bytes		5 895 568 410 ns	358 720 ns	FDT PCD to PICC = 774.68 ms	14443
5 896 100 360 ns	PCD_A	S(WTX) Response	4 bytes		5 896 468 520 ns	368 160 ns	FDT PICC to PCD = 541.3 µs	14443
6 671 115 850 ns	PICC_A	S(WTX) Request	4 bytes		6 671 474 570 ns	358 720 ns	FDT PCD to PICC = 774.66 ms	14443
6 671 997 120 ns	PCD_A	S(WTX) Response	4 bytes		6 672 365 280 ns	368 160 ns	FDT PICC to PCD = 532.1 µs	14443
7 447 012 790 ns	PICC_A	S(WTX) Request	4 bytes		7 447 371 490 ns	358 700 ns	FDT PCD to PICC = 774.66 ms	14443
7 447 893 360 ns	PCD_A	S(WTX) Response	4 bytes		7 448 271 520 ns	368 160 ns	FDT PICC to PCD = 541.4 µs	14443
8 216 352 920 ns	PCD_A	S(DESELECT)	3 bytes		8 216 636 120 ns	283 200 ns		14443

MP300-TCL2

- *Timeout* $\cong$ 624*ms*

Timeout=5s, Delay = 1s, R(NAK) after each 156ms = FWT, Reponse time = 1.020s

Start Date	Sender	Frame	Byte..	Error	End Date	Duration	Timing	Protocol
Protocol : 14443 - 16 item(s)								
4 939 002 600 ns	PCD_A	REQA	1 byte		4 939 097 000 ns	94 400 ns		14443
4 939 167 170 ns	PICC_A	ATQA	2 bytes		4 939 355 950 ns	188 780 ns	FDT PCD to PICC = 86.8 µs	14443
6 220 515 360 ns	PCD_A	ANTICOLLISION	2 bytes		6 220 713 580 ns	198 220 ns	FDT PICC to PCD = 1.28 s	14443
6 220 783 670 ns	PICC_A	UID CLn	5 bytes		6 221 227 330 ns	443 660 ns	FDT PCD to PICC = 86.7 µs	14443
6 221 349 200 ns	PCD_A	SELECT	9 bytes		6 222 142 120 ns	792 920 ns	FDT PICC to PCD = 119.2 µs	14443
6 222 212 210 ns	PICC_A	SAK	3 bytes		6 222 485 970 ns	273 760 ns	FDT PCD to PICC = 91.4 µs	14443
7 888 596 880 ns	PCD_A	RATS	4 bytes		7 888 965 020 ns	368 140 ns	FDT PICC to PCD = 1.67 s	14443
7 890 498 010 ns	PICC_A	ATS	8 bytes		7 891 196 530 ns	698 520 ns	FDT PCD to PICC = 1.55 ms	14443
13 212 073 180 ns	PCD_A	I(0)0	12 bytes	Invalid CID: CID not sent while it should have been.	13 213 120 960 ns	1 047 780 ns	FDT PICC to PCD = 5.32 s	14443
13 369 151 720 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	13 369 434 920 ns	283 200 ns		14443
13 525 442 820 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	13 525 726 000 ns	283 180 ns		14443
13 681 714 380 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	13 681 997 560 ns	283 180 ns		14443
13 838 024 200 ns	PCD_A	S(DESELECT)	3 bytes	Invalid CID: CID not sent while it should have been.	13 838 307 380 ns	283 180 ns		14443
13 994 317 580 ns	PCD_A	S(DESELECT)	3 bytes	Invalid CID: CID not sent while it should have been.	13 994 600 760 ns	283 180 ns		14443
14 150 586 760 ns	PCD_A	S(DESELECT)	3 bytes	Invalid CID: CID not sent while it should have been.	14 150 869 880 ns	283 180 ns		14443
14 234 039 010 ns	PICC_A	I(0)0	5 bytes	Invalid CID: CID not sent while it should have been.	14 234 482 670 ns	443 660 ns	FDT PCD to PICC = 83.19 ms	14443

Omnikey3521

- *Timeout* $= \infty$

Timeout = default, Delay = 2s, Response Time = 2,069s

Start Date	Sender	Frame	Byte...	Error	End Date	Duration	Timing	Protocol
105 626 416 600 ns	PCD_A	I(1)0	64 bytes		105 627 783 040 ns	1 366 440 ns	FDT PICC to PCD = 6.45 ms	14443
105 634 454 820 ns	PICC_A	R(ACK)0	4 bytes		105 634 539 860 ns	85 040 ns	FDT PCD to PICC = 6.64 ms	14443
105 635 693 360 ns	PCD_A	I(0)1	9 bytes		105 635 891 600 ns	198 240 ns	FDT PICC to PCD = 1.15 ms	14443
105 637 763 460 ns	PICC_A	S(WTX) Request	5 bytes		105 637 869 660 ns	106 200 ns	FDT PCD to PICC = 1.84 ms	14443
105 640 089 800 ns	PCD_A	S(WTX) Response	5 bytes		105 640 203 080 ns	113 280 ns	FDT PICC to PCD = 2.22 ms	14443
106 414 935 680 ns	PICC_A	S(WTX) Request	5 bytes		106 415 041 880 ns	106 200 ns	FDT PCD to PICC = 774.7 ms	14443
106 416 318 240 ns	PCD_A	S(WTX) Response	5 bytes		106 416 431 520 ns	113 280 ns	FDT PICC to PCD = 1.28 ms	14443
107 191 060 420 ns	PICC_A	S(WTX) Request	5 bytes		107 191 166 600 ns	106 180 ns	FDT PCD to PICC = 774.59 ms	14443
107 192 324 800 ns	PCD_A	S(WTX) Response	5 bytes		107 192 438 080 ns	113 280 ns	FDT PICC to PCD = 1.16 ms	14443
107 704 479 920 ns	PICC_A	I(0)1	6 bytes		107 704 607 360 ns	127 440 ns	FDT PCD to PICC = 512.01 ms	14443
107 708 262 320 ns	PCD_A	I(1)0	64 bytes		107 709 628 760 ns	1 366 440 ns	FDT PICC to PCD = 3.65 ms	14443
107 716 826 720 ns	PICC_A	R(ACK)0	4 bytes		107 716 911 660 ns	84 940 ns	FDT PCD to PICC = 7.16 ms	14443
107 717 973 240 ns	PCD_A	I(0)1	9 bytes		107 718 171 480 ns	198 240 ns	FDT PICC to PCD = 1.06 ms	14443
107 720 045 680 ns	PICC_A	S(WTX) Request	5 bytes		107 720 151 860 ns	106 180 ns	FDT PCD to PICC = 1.84 ms	14443
107 722 117 200 ns	PCD_A	S(WTX) Response	5 bytes		107 722 230 480 ns	113 280 ns	FDT PICC to PCD = 1.97 ms	14443
108 496 963 180 ns	PICC_A	S(WTX) Request	5 bytes		108 497 069 380 ns	106 200 ns	FDT PCD to PICC = 774.7 ms	14443
108 498 303 160 ns	PCD_A	S(WTX) Response	5 bytes		108 498 416 440 ns	113 280 ns	FDT PICC to PCD = 1.23 ms	14443
109 273 045 280 ns	PICC_A	S(WTX) Request	5 bytes		109 273 151 460 ns	106 180 ns	FDT PCD to PICC = 774.59 ms	14443
109 274 354 560 ns	PCD_A	S(WTX) Response	5 bytes		109 274 467 840 ns	113 280 ns	FDT PICC to PCD = 1.2 ms	14443
109 788 527 260 ns	PICC_A	I(0)1	6 bytes		109 788 654 700 ns	127 440 ns	FDT PCD to PICC = 514.02 ms	14443

Hancke : Relay attack on ISO14443 type A cards I

- Terminology :
  - Mole = fake reader, Proxy = fake tag.
  - Reader = legitimate reader, Card = legitimate tag.
- Tools :
  - They use dedicated hardware to make the mole and the proxy.
  - They are interested in how to relay anti-collision commands with a minimum delay.
- Results :
  - Distance *Mole* $\leftrightarrow$ *Card* : 10cm.
  - Distance *Proxy* $\leftrightarrow$ *Reader* : 10cm.
  - Distance *Mole* $\leftrightarrow$ *Proxy* : 50m.
  - Delay time : 15 - 20 us.

Kfir and Wool : Relay attack on ISO14443 type B cards I

- Terminology :
  - Leech = fake reader, Ghost = fake tag.
  - Reader = legitimate reader, Tag = legitimate tag.
- Tools : hardware and software tools that require a very high to medium attacker knowledge and cost between 100$ and 5000$.
- Results :
  - Distance *Ghost* $\leftrightarrow$ *Reader* : 50m
    - Communication *Reader* $\rightarrow$ *Ghost* : they use an active tag.
    - Communication *Ghost* $\rightarrow$ *Reader* : they use the DSB modulation.

Kfir and Wool : Relay attack on ISO14443 type B cards II

- Distance *Leech* $\leftrightarrow$ *Tag* : 40 - 55 cm
  - Communication *Leech* $\rightarrow$ *Tag* : Current(4A) + Antenna ($40 * 40 cm^2$).
  - Communication *Tag* $\rightarrow$ *Leech* :
    - Nothing (40 cm)
    - Software based retransmissions (50 cm).
    - Signal Based retransmissions (55 cm).
- Distance *Leech* $\leftrightarrow$ *Ghost* : not studied.

Francillon : Relay attack on PKES I

- Principle :
  - The messages related to the authentication process are relayed from the car to the key and not from the key to the car, because the car sends messages through a LF channel while the key sends messages through a UHF channel.
  - Two types of attack were proposed : wireless relay attack, and wired relay attack.
- Wired relay attack :
  - Tools: Coaxial cable, 2 antennas, 2 optional amplifiers.
  - Results :
    - Distance $Antenna1 \leftrightarrow Car : \leq 30cm$.
    - Distance $Antenna2 \leftrightarrow Key : \leq 2m$ without the amplifier and $\leq 8m$ with the amplifier.

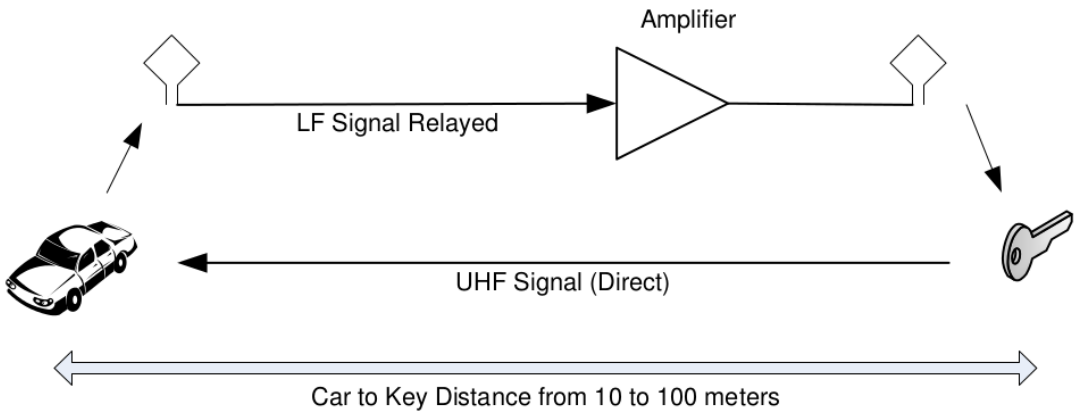
Francillon : Relay attack on PKES II

- Distance *Car* $\rightarrow$ *Key* : up to 60m.
- Distance *Key* $\rightarrow$ *Car* : up to 100m.
- Delay : it only includes the propagation delay since the attack doesn't perform any additional operations.
  - Delay *Car* $\rightarrow$ *Key* : 350ns.
  - Delay *Key* $\rightarrow$ *Car* : depends only on the distance between the key and the car.

- Wirless relay attack :
  - Tools: 2 antennas, emitter, receiver, amplifier.
  - Results :
    - Distance *Antenna*1 $\leftrightarrow$ *Car* : $\leq 30cm$.
    - Distance *Antenna*2 $\leftrightarrow$ *Key* : $\leq 2m$ without the amplifier and $\leq 8m$ with the amplifier.
    - Distance *Car* $\rightarrow$ *Key* : 30m, but bigger distances may be possible..

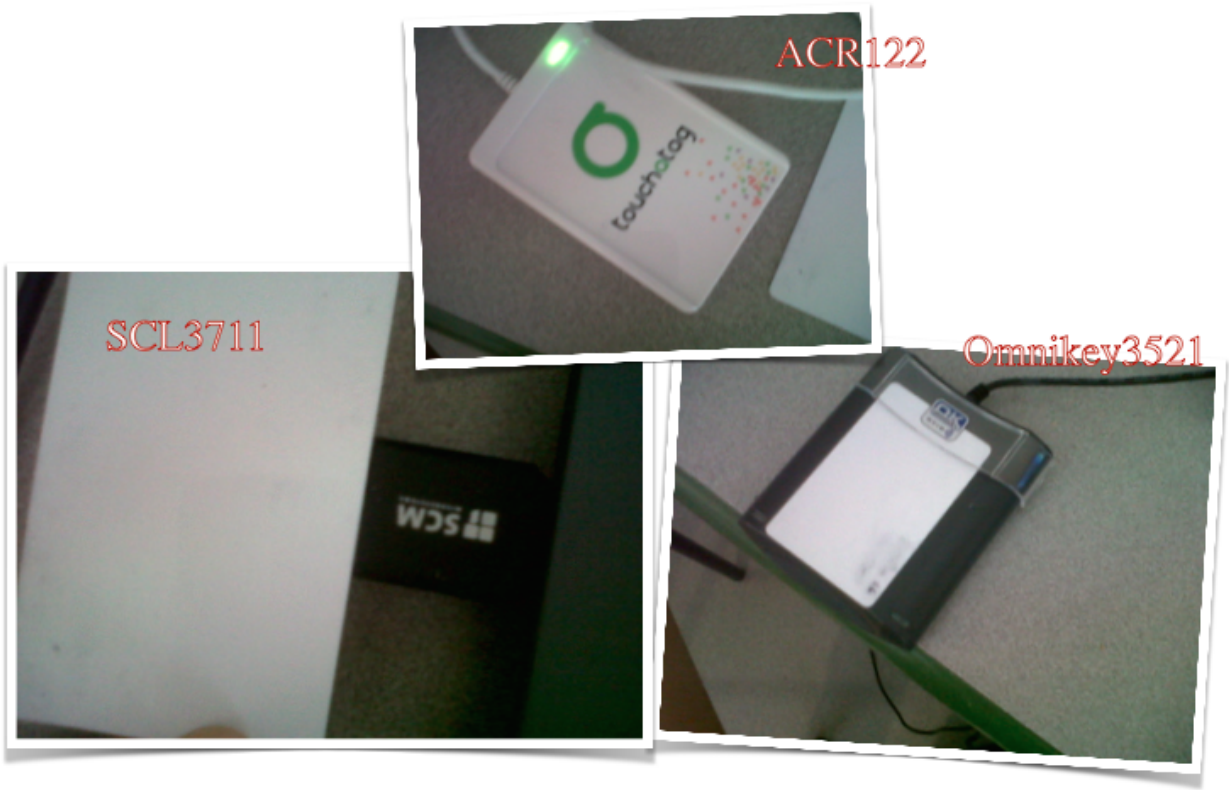
Francillon : Relay attack on PKES III

- Distance *Key* $\rightarrow$ *Car* : up to 100m.
- Delay *Car* $\rightarrow$ *Key* :120ns.
- Delay *Key* $\rightarrow$ *Car* : depends only on the distance between the key and the car.



Microprocess

Other Readers

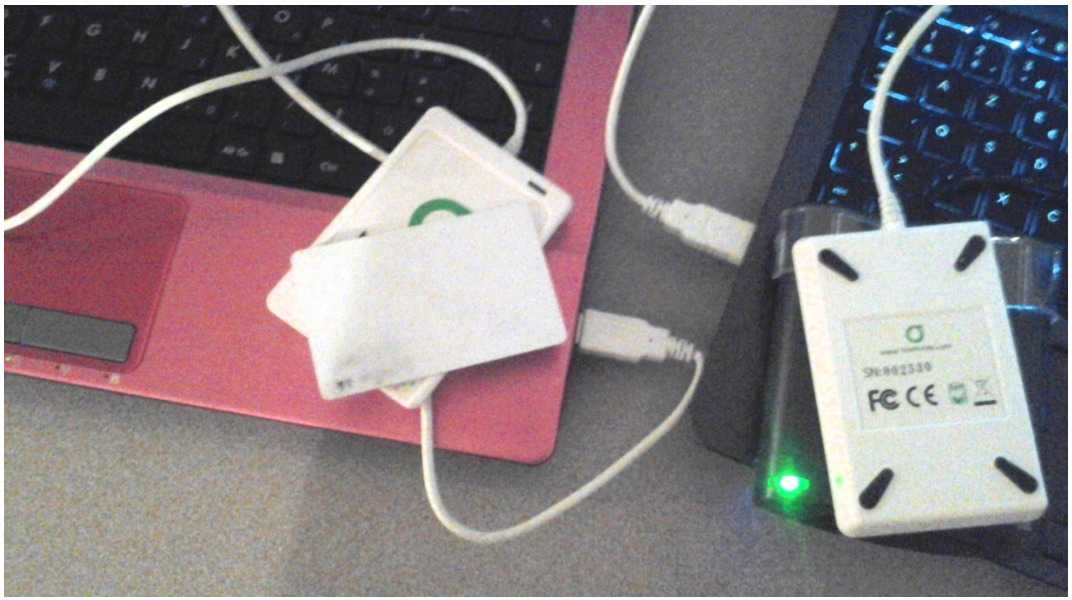


Softwares

- LibNfc to program the ACR122 and SCL3711 readers.
- PCSC libraries to program the Omnikey5321 reader.
- Microprossx APIs to program the MP300 - TCL2 reader.

Context

- ACR122, or SCL3711, or Omnikey3521, or TCL2 : legitimate reader.
- ACR122 : fake tag (ISO14443-4 A card emulation).
- Mifare Desfire : legitimate tag.
- ACR122 : fake reader.



Demo

Fake Reader and legitimate Tag
Legitemate Reader and fake Tag

Experiment 1 I

- Goal : Does the command size, or the response size or the data size influence the response time of the card ?
- Answer : No, they don't
- Proof :

Experiment 1 II

	Data Size W	Data Size R	Command Size	Response Size	Response Time(us)
REQA					86
AntiColl					86
SelectRootApp			9	2	841
ListApps1			5	2	841
ListApps2			0	0	0
getKeySettings_Delete			0	0	0
authPass1_Delete			0	0	0
authPass2_Delete			0	0	0
deleteApp			0	0	0
CreateApp			11	2	4315
[illegible]			9	2	841
CreateFilePlain (1 Ko)			13	2	20853
CreateFileMac (1 Ko)			13	2	23798
CreateFileEncr (1 Ko)			13	2	19191
getkeySettings_CK			5	4	463
authPass1_CK			7	10	846
authPass2_CK			22	10	846
ChangeKey			31	2	18814
authPass1_WR			7	10	846
authPass2_WR			22	10	921
writePlain1	0x60		65	2	4244
writePlain2			50	2	3866
writeEncry1	0x60		65	2	4817
writeEncry2			58	2	8090
writeMac1	0x60		65	2	3413
writeMac2			54	2	7113
readPlain1		0x60	13	2	166
readPlain2			6	39	770
readMac1		0x60	13	58	2578
readMac2			6	46	1601
readEncry1		0x60	13	58	3111
readEncry2			6	50	2205
listFiles			5	5	765
deleteFile1			6	2	9077
deleteFile2			6	2	9148
deleteFile3			6	2	9223
selectApp_reset			9	2	463
authPass1_reset			7	10	695
authPass2_reset			22	10	841
reset			5	2	11720

Experiment 1 III

	Data_Size_W	Data_Size_R	N = 0.7	Data_Size_W	Data_Size_R	N = 0.7
SelectRootApp			OK			OK
ListApps1			OK			OK
ListApps2						
getKeySettings_Delete			OK			OK
authPass1_Delete			OK			OK
authPass2_Delete			OK			OK
deleteApp			OK			OK
CreateApp			OK			OK
selectApp_aid2			OK			OK
CreateFilePlain (1 Ko)			OK			OK
CreateFileMac (1 Ko)			OK			OK
CreateFileEncr (1 Ko)			OK			OK
getkeySettings_CK			OK			OK
authPass1_CK			OK			OK
authPass2_CK			OK			OK
ChangeKey			OK			OK
authPass1_WR			OK			OK
authPass2_WR			OK			OK
writePlain1	0x28		OK	0x2D		OK
writePlain2			OK			OK
writeMac1	0x28		OK	0x2D		OK
writeMac2			OK			OK
writeEncry1	0x28		OK	0x2D		OK
writeEncry2			OK			OK
readPlain1		0x28	OK		0x2D	OK
readPlain2			OK			OK
readMac1		0x28	OK		0x2D	OK
readMac2			OK			OK
readEncry1		0x28	KO		0x2D	OK
readEncry2						OK
listFiles						OK
deleteFile1						OK
deleteFile2						OK
deleteFile3						OK
selectApp_reset						OK
authPass1_reset						OK
authPass2_reset						OK
reset						OK

Experiment 1bis I

- Goal : Does the card emulation influence the response time of the card ? and what is the magnitude of the propagation time ?
- Answer :
  - Yes, the card emulation impacts the response time of the card.
  - The transmission time is not very significant compared to the processing time.
- Proof :

Experiment 1bis II

	Data Size W	Data Size R	Command Size	Response Size	Response Time(us)
REQA					86
AntiColl					91
SelectRootApp			9	2	20820
ListApps1			5	2	18918
ListApps2			0	0	0
getKeySettings_Delete			0	0	0
authPass1_Delete			0	0	0
authPass2_Delete			0	0	0
deleteApp			0	0	0
CreateApp			11	2	51971
			9	2	21080
selectApp_aid2			23	11	
CreateFilePlain (1 Ko)			13	2	74895
CreateFileMac (1 Ko)			13	2	76556
CreateFileEncr (1 Ko)			13	2	74102
getkeySettings_CK			5	4	19338
authPass1_CK			7	10	24502
authPass2_CK			22	10	33545
ChangeKey			31	2	44353
authPass1_WR			7	10	24105
authPass2_WR			22	10	33469
writePlain1	0x60		65	2	55997
writePlain2			50	2	49247
writeEncry1	0x60		65	2	55539
writeEncry2			58	2	58588
writeMac1	0x60		65	2	55331
writeMac2			54	2	55213
readPlain1		0x60	13	2	60042
readPlain2			6	39	39657
readMac1		0x60	13	58	57738
readMac2			6	46	44518
readEncry1		0x60	13	58	58394
readEncry2			6	50	47888
listFiles			5	5	19909
deleteFile1			6	2	27428
deleteFile2			6	2	27555
deleteFile3			6	2	27688
selectApp_reset			9	2	20018
authPass1_reset			7	10	23709
authPass2_reset			22	10	33139

Experiment 1bis III

Response Time = 0.628s, processing time = 20820us => Processing time + Propagation time = 0.28s => Propagation time =7180us.

8 265 031 150 ns	PICC_A	ATS	8 bytes	8 265 729 650 ns	698 500 ns	FDT PCD to PICC = 1.56 ms	14443
8 283 525 780 ns	PCD_A	I(0)0	12 bytes	8 284 573 620 ns	1 047 840 ns	FDT PICC to PCD = 17.81 ms	14443
8 286 693 450 ns	PICC_A	S(WTX) Request	4 bytes	8 287 052 150 ns	358 700 ns	FDT PCD to PICC = 2.14 ms	14443
8 288 546 700 ns	PCD_A	S(WTX) Response	4 bytes	8 288 914 860 ns	368 160 ns	FDT PICC to PCD = 1.5 ms	14443
8 913 316 090 ns	PICC_A	I(0)0	5 bytes	8 913 759 730 ns	443 640 ns	FDT PCD to PICC = 624.42 ms	14443
8 925 014 540 ns	PCD_A	I(0)1	8 bytes	8 925 722 540 ns	708 000 ns	FDT PICC to PCD = 11.26 ms	14443

Experiment 2 I

- Goal : Acceptable delays by the ACR122 reader when doing relay attack against the Mifare Desfire.
- Results :
  - Timeout = default : 0.6s for all the commands we have tested and 0.7s for someones.
  - Timeout = 5s : 4.7s for all the commands we have tested.
- Proof :

Experiment 2 II

	N = 0	N = 0.5	N = 0.6	N = 0.7	N =0.8
SelectRootApp	OK	OK	OK	OK	KO
ListApps1	OK	OK	OK	OK	
ListApps2	OK	OK	OK	OK	
getKeySettings_Delete	OK	OK	OK	OK	
authPass1_Delete	OK	OK	OK	OK	
authPass2_Delete	OK	OK	OK	OK	
deleteApp	OK	OK	OK	OK	
CreateApp	OK	OK	OK	OK	
selectApp_aid2	OK	OK	OK	OK	
CreateFilePlain (1 Ko)	OK	OK	OK	OK	
CreateFileMac (1 Ko)	OK	OK	OK	OK	
CreateFileEncr (1 Ko)	OK	OK	OK	OK	
getkeySettings_CK	OK	OK	OK	OK	
authPass1_CK	OK	OK	OK	OK	
authPass2_CK	OK	OK	OK	OK	
ChangeKey	OK	OK	OK	OK	
authPass1_WR	OK	OK	OK	OK	
authPass2_WR	OK	OK	OK	OK	
writePlain1	OK	OK	OK	KO	
writePlain2	OK	OK	OK		
writeEncry1	OK	OK	OK		
writeEncry2	OK	OK	OK		
writeMac1	OK	OK	OK		
writeMac2	OK	OK	OK		
readPlain1	OK	OK	OK		
readPlain2	OK	OK	OK		
readMac1	OK	OK	OK		
readMac2	OK	OK	OK		
readEncry1	OK	OK	OK		
readEncry2	OK	OK	OK		
listFiles	OK	OK	OK		
deleteFile1	OK	OK	OK		
deleteFile2	OK	OK	OK		
deleteFile3	OK	OK	OK		
selectApp_reset	OK	OK	OK		
authPass1_reset	OK	OK	OK		
authPass2_reset	OK	OK	OK		

Experiment 2 III

	N = 0	N = 3	N = 4	N = 4,5	N = 4,6	N = 4,7	N = 4,8
SelectRootApp	OK	OK	OK	OK	OK	OK	KO
ListApps1	OK	OK	OK	OK	OK	OK	
ListApps2	OK	OK	OK	OK	OK	OK	
getKeySettings_Delete	OK	OK	OK	OK	OK	OK	
authPass1_Delete	OK	OK	OK	OK	OK	OK	
authPass2_Delete	OK	OK	OK	OK	OK	OK	
deleteApp	OK	OK	OK	OK	OK	OK	
CreateApp	OK	OK	OK	OK	OK	OK	
selectApp_aid2	OK	OK	OK	OK	OK	OK	
CreateFilePlain (1 Ko)	OK	OK	OK	OK	OK	OK	
CreateFileMac (1 Ko)	OK	OK	OK	OK	OK	OK	
CreateFileEncr (1 Ko)	OK	OK	OK	OK	OK	OK	
getkeySettings_CK	OK	OK	OK	OK	OK	OK	
authPass1_CK	OK	OK	OK	OK	OK	OK	
authPass2_CK	OK	OK	OK	OK	OK	OK	
ChangeKey	OK	OK	OK	OK	OK	OK	
authPass1_WR	OK	OK	OK	OK	OK	OK	
authPass2_WR	OK	OK	OK	OK	OK	OK	
writePlain1	OK	OK	OK	OK	OK	OK	
writePlain2	OK	OK	OK	OK	OK	OK	
writeEncry1	OK	OK	OK	OK	OK	OK	
writeEncry2	OK	OK	OK	OK	OK	OK	
writeMac1	OK	OK	OK	OK	OK	OK	
writeMac2	OK	OK	OK	OK	OK	OK	
readPlain1	OK	OK	OK	OK	OK	OK	
readPlain2	OK	OK	OK	OK	OK	OK	
readMac1	OK	OK	OK	OK	OK	OK	
readMac2	OK	OK	OK	OK	OK	OK	
readEncry1	OK	OK	OK	OK	OK	OK	
readEncry2	OK	OK	OK	OK	OK	OK	
listFiles	OK	OK	OK	OK	OK	OK	
deleteFile1	OK	OK	OK	OK	OK	OK	
deleteFile2	OK	OK	OK	OK	OK	OK	
deleteFile3	OK	OK	OK	OK	OK	OK	
selectApp_reset	OK	OK	OK	OK	OK	OK	
authPass1_reset	OK	OK	OK	OK	OK	OK	
authPass2_reset	OK	OK	OK	OK	OK	OK	

Experiment 2 IV

Timeout = Default, Delay = 0.8s , Response time = 0.83s

5 970 687 580 ns	PCD_A	REQA	1 byte		5 970 781 980 ns	94 400 ns		14443
5 970 853 630 ns	PICC_A	ATQA	2 bytes		5 971 042 430 ns	188 800 ns	FDT PCD to PICC = 87.5 µs	14443
5 971 668 500 ns	PCD_A	ANTICOLLISION	2 bytes		5 971 866 740 ns	198 240 ns	FDT PICC to PCD = 640.5 µs	14443
5 971 938 350 ns	PICC_A	UID CLn	5 bytes		5 972 381 990 ns	443 640 ns	FDT PCD to PICC = 87.4 µs	14443
5 973 942 660 ns	PCD_A	SELECT	9 bytes		5 974 735 620 ns	792 960 ns	FDT PICC to PCD = 1.57 ms	14443
5 974 807 210 ns	PICC_A	SAK	3 bytes		5 975 080 950 ns	273 740 ns	FDT PCD to PICC = 87.5 µs	14443
5 975 678 740 ns	PCD_A	RATS	4 bytes		5 976 046 900 ns	368 160 ns	FDT PICC to PCD = 607.5 µs	14443
5 977 591 050 ns	PICC_A	ATS	8 bytes		5 978 289 550 ns	698 500 ns	FDT PCD to PICC = 1.56 ms	14443
5 996 104 540 ns	PCD_A	I(0)0	12 bytes		5 997 152 380 ns	1 047 840 ns	FDT PICC to PCD = 17.83 ms	14443
5 999 272 150 ns	PICC_A	S(WTX) Request	4 bytes		5 999 630 850 ns	358 700 ns	FDT PCD to PICC = 2.14 ms	14443
6 001 125 500 ns	PCD_A	S(WTX) Response	4 bytes		6 001 493 660 ns	368 160 ns	FDT PICC to PCD = 1.5 ms	14443
6 776 054 210 ns	PICC_A	S(WTX) Request	4 bytes		6 776 412 910 ns	358 700 ns	FDT PCD to PICC = 774.58 ms	14443
6 778 398 380 ns	PCD_A	S(WTX) Response	4 bytes		6 778 766 540 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
6 827 752 170 ns	PICC_A	I(0)0	5 bytes		6 828 195 810 ns	443 640 ns	FDT PCD to PICC = 49 ms	14443
[illegible]	PCD_A	S(DESELECT)	3 bytes		6 838 969 300 ns	283 200 ns	FDT PICC to PCD = 10.5 ms	14443
6 839 474 870 ns	PICC_A	S(DESELECT)	3 bytes		6 839 748 610 ns	273 740 ns	FDT PCD to PICC = 526.2 µs	14443

Experiment 2 V

Timeout = 5s, Delay = 5s, Response time = 5.028s

Start Date	Sender	Frame	Byte...	Error	End Date	Duration	Timing	Protocol
7 474 487 640 ns	PCD_A	REQA	1 byte		7 474 582 040 ns	94 400 ns		14443
7 474 653 630 ns	PICC_A	ATQA	2 bytes		7 474 842 410 ns	188 780 ns	FDT PCD to PICC = 87.4 µs	14443
7 475 468 600 ns	PCD_A	ANTICOLLISION	2 bytes		7 475 666 840 ns	198 240 ns	FDT PICC to PCD = 640.6 µs	14443
7 475 738 390 ns	PICC_A	UID CLn	5 bytes		7 476 182 050 ns	443 660 ns	FDT PCD to PICC = 87.4 µs	14443
7 477 742 720 ns	PCD_A	SELECT	9 bytes		7 478 535 680 ns	792 960 ns	FDT PICC to PCD = 1.57 ms	14443
7 478 607 190 ns	PICC_A	SAK	3 bytes		7 478 880 930 ns	273 740 ns	FDT PCD to PICC = 87.4 µs	14443
7 479 478 800 ns	PCD_A	RATS	4 bytes		7 479 846 960 ns	368 160 ns	FDT PICC to PCD = 607.6 µs	14443
7 481 381 650 ns	PICC_A	ATS	8 bytes		7 482 080 170 ns	698 520 ns	FDT PCD to PICC = 1.56 ms	14443
7 499 829 040 ns	PCD_A	I(0)0	12 bytes		7 500 876 880 ns	1 047 840 ns	FDT PICC to PCD = 17.76 ms	14443
7 502 996 690 ns	PICC_A	S(WTX) Request	4 bytes		7 503 368 390 ns	358 700 ns	FDT PCD to PICC = 2.14 ms	14443
7 504 850 000 ns	PCD_A	S(WTX) Response	4 bytes		7 505 218 160 ns	368 160 ns	FDT PICC to PCD = 1.5 ms	14443
8 279 778 910 ns	PICC_A	S(WTX) Request	4 bytes		8 280 137 610 ns	358 700 ns	FDT PCD to PICC = 774.58 ms	14443
8 282 123 040 ns	PCD_A	S(WTX) Response	4 bytes		8 282 491 200 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
9 057 042 530 ns	PICC_A	S(WTX) Request	4 bytes		9 057 401 210 ns	358 680 ns	FDT PCD to PICC = 774.57 ms	14443
9 059 386 640 ns	PCD_A	S(WTX) Response	4 bytes		9 059 754 800 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
9 834 306 150 ns	PICC_A	S(WTX) Request	4 bytes		9 834 664 830 ns	358 680 ns	FDT PCD to PICC = 774.57 ms	14443
9 836 650 280 ns	PCD_A	S(WTX) Response	4 bytes		9 837 018 440 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
10 611 569 830 ns	PICC_A	S(WTX) Request	4 bytes		10 611 928 530 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
10 613 913 920 ns	PCD_A	S(WTX) Response	4 bytes		10 614 282 080 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
11 388 833 370 ns	PICC_A	S(WTX) Request	4 bytes		11 389 192 070 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
11 391 177 520 ns	PCD_A	S(WTX) Response	4 bytes		11 391 545 680 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
12 166 096 990 ns	PICC_A	S(WTX) Request	4 bytes		12 166 455 690 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
12 168 441 120 ns	PCD_A	S(WTX) Response	4 bytes		12 168 809 280 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
12 529 610 710 ns	PICC_A	I(0)0	5 bytes		12 530 054 350 ns	443 640 ns	FDT PCD to PICC = 360.82 ms	14443
12 540 478 400 ns	PCD_A	S(DESELECT)	3 bytes		12 540 761 600 ns	283 200 ns	FDT PICC to PCD = 10.43 ms	14443
12 541 267 350 ns	PICC_A	S(DESELECT)	3 bytes		12 541 541 090 ns	273 740 ns	FDT PCD to PICC = 526.3 µs	14443

Experiment 2 VI

Timeout = 5s, Delay = 4.6s

12 237 790 650 ns	PICC_A	ATS	8 bytes	12 238 489 150 ns	698 500 ns	FDT PCD to PICC = 1.56 ms	14443
12 256 776 180 ns	PCD_A	I(0)0	12 bytes	12 257 824 020 ns	1 047 840 ns	FDT PICC to PCD = 18.3 ms	14443
12 259 953 290 ns	PICC_A	S(WTX) Request	4 bytes	12 260 311 970 ns	358 680 ns	FDT PCD to PICC = 2.15 ms	14443
12 261 806 700 ns	PCD_A	S(WTX) Response	4 bytes	12 262 174 860 ns	368 160 ns	FDT PICC to PCD = 1.5 ms	14443
13 039 079 100 ns	PCD_A	S(WTX) Response	4 bytes	13 039 447 260 ns	368 160 ns		14443
13 813 997 910 ns	PICC_A	S(WTX) Request	4 bytes	13 814 356 610 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
13 816 342 140 ns	PCD_A	S(WTX) Response	4 bytes	13 816 710 300 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
14 591 260 750 ns	PICC_A	S(WTX) Request	4 bytes	14 591 619 450 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
14 593 605 100 ns	PCD_A	S(WTX) Response	4 bytes	14 593 973 260 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
15 368 523 950 ns	PICC_A	S(WTX) Request	4 bytes	15 368 882 650 ns	358 700 ns	FDT PCD to PICC = 774.57 ms	14443
15 370 868 100 ns	PCD_A	S(WTX) Response	4 bytes	15 371 236 260 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
16 145 786 870 ns	PICC_A	S(WTX) Request	4 bytes	16 146 145 550 ns	358 680 ns	FDT PCD to PICC = 774.57 ms	14443
16 148 131 060 ns	PCD_A	S(WTX) Response	4 bytes	16 148 499 220 ns	368 160 ns	FDT PICC to PCD = 2 ms	14443
16 886 614 430 ns	PICC_A	I(0)0	5 bytes	16 887 058 090 ns	443 660 ns	FDT PCD to PICC = 738.13 ms	14443

Experiment 3 I

- Goal : Acceptable delays by the SCL3711 reader when doing relay attack against the Mifare Desfire.
- Results :
  - Timeout = default : 0s .
  - Timeout = 5s : 4.7s for all the commands we have tested.
- Proof :

Experiment 3 II

	N = 0	N = 3	N = 4	N = 4,5	N = 4,6	N = 4,7	N = 4,8
SelectRootApp	OK	OK	OK	OK	OK	OK	KO
ListApps1	OK	OK	OK	OK	OK	OK	
ListApps2	OK	OK	OK	OK	OK	OK	
getKeySettings_Delete	OK	OK	OK	OK	OK	OK	
authPass1_Delete	OK	OK	OK	OK	OK	OK	
authPass2_Delete	OK	OK	OK	OK	OK	OK	
deleteApp	OK	OK	OK	OK	OK	OK	
CreateApp	OK	OK	OK	OK	OK	OK	
selectApp_aid2	OK	OK	OK	OK	OK	OK	
CreateFilePlain (1 Ko)	OK	OK	OK	OK	OK	OK	
CreateFileMac (1 Ko)	OK	OK	OK	OK	OK	OK	
CreateFileEncr (1 Ko)	OK	OK	OK	OK	OK	OK	
getkeySettings_CK	OK	OK	OK	OK	OK	OK	
authPass1_CK	OK	OK	OK	OK	OK	OK	
authPass2_CK	OK	OK	OK	OK	OK	OK	
ChangeKey	OK	OK	OK	OK	OK	OK	
authPass1_WR	OK	OK	OK	OK	OK	OK	
authPass2_WR	OK	OK	OK	OK	OK	OK	
writePlain1	OK	OK	OK	OK	OK	OK	
writePlain2	OK	OK	OK	OK	OK	OK	
writeEncry1	OK	OK	OK	OK	OK	OK	
writeEncry2	OK	OK	OK	OK	OK	OK	
writeMac1	OK	OK	OK	OK	OK	OK	
writeMac2	OK	OK	OK	OK	OK	OK	
readPlain1	OK	OK	OK	OK	OK	OK	
readPlain2	OK	OK	OK	OK	OK	OK	
readMac1	OK	OK	OK	OK	OK	OK	
readMac2	OK	OK	OK	OK	OK	OK	
readEncry1	OK	OK	OK	OK	OK	OK	
readEncry2	OK	OK	OK	OK	OK	OK	
listFiles	OK	OK	OK	OK	OK	OK	
deleteFile1	OK	OK	OK	OK	OK	OK	
deleteFile2	OK	OK	OK	OK	OK	OK	
deleteFile3	OK	OK	OK	OK	OK	OK	
selectApp_reset	OK	OK	OK	OK	OK	OK	
authPass1_reset	OK	OK	OK	OK	OK	OK	
authPass2_reset	OK	OK	OK	OK	OK	OK	
reset	OK	OK	OK	OK	OK	OK	

Experiment 3 III

Timeout = Default, Delay = 0.2s , S(DESELECT) after 0.158s

6 745 002 620 ns	PCD_A	REQA	1 byte	6 745 097 020 ns	94 400 ns		14443
6 745 168 570 ns	PICC_A	ATQA	2 bytes	6 745 357 370 ns	188 800 ns	FDT PCD to PICC = 87.3 µs	14443
6 745 549 380 ns	PCD_A	ANTICOLLISION	2 bytes	6 745 747 620 ns	198 240 ns	FDT PICC to PCD = 206.3 µs	14443
6 745 819 330 ns	PICC_A	UID CLn	5 bytes	6 746 262 990 ns	443 660 ns	FDT PCD to PICC = 87.5 µs	14443
6 747 427 580 ns	PCD_A	SELECT	9 bytes	6 748 220 540 ns	792 960 ns	FDT PICC to PCD = 1.17 ms	14443
6 748 292 170 ns	PICC_A	SAK	3 bytes	6 748 565 910 ns	273 740 ns	FDT PCD to PICC = 87.4 µs	14443
6 749 466 260 ns	PCD_A	RATS	4 bytes	6 749 834 420 ns	368 160 ns	FDT PICC to PCD = 909.9 µs	14443
6 751 359 710 ns	PICC_A	ATS	8 bytes	[illegible]	698 540 ns	FDT PCD to PICC = 1.54 ms	14443
6 757 451 700 ns	PCD_A	I(0)0	12 bytes	6 758 499 540 ns	1 047 840 ns	FDT PICC to PCD = 5.41 ms	14443
6 760 619 630 ns	PICC_A	S(WTX) Request	4 bytes	6 760 978 330 ns	358 700 ns	FDT PCD to PICC = 2.14 ms	14443
6 761 378 300 ns	PCD_A	S(WTX) Response	4 bytes	6 761 746 460 ns	368 160 ns	FDT PICC to PCD = 409.6 µs	14443
6 916 793 780 ns	PCD_A	S(DESELECT)	3 bytes	6 917 076 980 ns	283 200 ns		14443

Experiment 4 I

- Goal : Acceptable delays by the Omnikey3521 reader when doing relay attack against the Mifare Desfire.
- Results :
  - Timeout = default : ∞ .
  - Timeout = 5s : 4s for all the commands we have tested.

Experiment 5 I

- Goal : Acceptable delays by the MP300-TCL2 reader when doing relay attack against the Mifare Desfire.
- Results :
  - Timeout = default : 0.5s for all the commands we have tested and 0.6s for someones.
  - Timeout = 5s : 0.5s for all the commands we have tested and 0.6s for someones.
- Proof :

Experiment 5 II

	N = 0	N = 0.5	N = 0.6	N = 0.7	N = 0.6
SelectRootApp	OK	OK	OK	KO	OK
ListApps1	OK	OK	OK		OK
ListApps2	OK	OK			
getKeySettings_Delete	OK	OK			OK
authPass1_Delete	OK	OK			KO
authPass2_Delete	OK	OK			
deleteApp	OK	OK			
CreateApp	OK	OK	KO		
selectApp_aid2	OK	OK			
CreateFilePlain (1 Ko)	OK	OK			
CreateFileMac (1 Ko)	OK	OK			
CreateFileEncr (1 Ko)	OK	OK			
getkeySettings_CK	OK	OK			
authPass1_CK	OK	OK			
authPass2_CK	OK	OK			
ChangeKey	OK	OK			
authPass1_WR	OK	OK			
authPass2_WR	OK	OK			
writePlain1	OK	OK			
writePlain2	OK	OK			
writeEncry1	OK	OK			
writeEncry2	OK	OK			
writeMac1	OK	OK			
writeMac2	OK	OK			
readPlain1	OK	OK			
readPlain2	OK	OK			
readMac1	OK	OK			
readMac2	OK	OK			
readEncry1	OK	OK			
readEncry2	OK	OK			
listFiles	OK	OK			
deleteFile1	OK	OK			
deleteFile2	OK	OK			
deleteFile3	OK	OK			
selectApp_reset	OK	OK			
authPass1_reset	OK	OK			
authPass2_reset	OK	OK			
reset	OK	OK			

Experiment 5 III

Timeout = Default, TCL2 reader , Mifare Desfire card

726 887 110 ns	PICC_A	ATS	8 bytes		727 585 650 ns	698 540 ns	FDT PCD to PICC = 86.1 µs	14443
731 356 920 ns	PCD_A	I(0)0	13 bytes		732 489 680 ns	1 132 760 ns	FDT PICC to PCD = 3.78 ms	14443
733 314 410 ns	PICC_A	I(0)0	6 bytes		733 843 030 ns	528 620 ns	FDT PCD to PICC = 841.4 µs	14443
740 318 360 ns	PCD_A	I(0)1	9 bytes		741 111 280 ns	792 920 ns	FDT PICC to PCD = 6.49 ms	14443
741 633 810 ns	PICC_A	I(0)1	6 bytes		742 162 410 ns	528 600 ns	FDT PCD to PICC = 543.9 µs	14443
747 767 540 ns	PCD_A	I(0)0	15 bytes		749 070 200 ns	1 302 660 ns	FDT PICC to PCD = 5.62 ms	14443
772 927 310 ns	PICC_A	S(WTX) Request	5 bytes		773 370 970 ns	443 660 ns	FDT PCD to PICC = 23.87 ms	14443
773 581 340 ns	PCD_A	S(WTX) Response	5 bytes		774 034 440 ns	453 100 ns	FDT PICC to PCD = 220.1 µs	14443
778 332 850 ns	PICC_A	I(0)0	6 bytes		778 861 470 ns	528 620 ns	FDT PCD to PICC = 4.32 ms	14443
786 586 580 ns	PCD_A	I(0)1	13 bytes		787 719 320 ns	1 132 740 ns	FDT PICC to PCD = 7.73 ms	14443

Experiment 5 IV

Timeout = 5s, Delay = 0.5s

5 728 198 490 ns	PICC_A	ATQA	2 bytes		5 728 387 270 ns	188 780 ns	FDT PCD to PICC = 86.7 µs	14443
8 386 801 160 ns	PCD_A	ANTICOLLISION	2 bytes		8 386 999 400 ns	198 240 ns	FDT PICC to PCD = 2.66 s	14443
8 387 069 410 ns	PICC_A	UID CLn	5 bytes		8 387 513 070 ns	443 660 ns	FDT PCD to PICC = 86.7 µs	14443
8 389 496 600 ns	PCD_A	SELECT	9 bytes		8 390 289 520 ns	792 920 ns	FDT PICC to PCD = 1.98 ms	14443
8 390 359 310 ns	PICC_A	SAK	3 bytes		8 390 633 050 ns	273 740 ns	FDT PCD to PICC = 91.2 µs	14443
10 307 753 580 ns	PCD_A	RATS	4 bytes		10 308 121 720 ns	368 140 ns	FDT PICC to PCD = 1.92 s	14443
10 309 645 510 ns	PICC_A	ATS	8 bytes		10 310 344 030 ns	698 520 ns	FDT PCD to PICC = 1.54 ms	14443
18 700 927 100 ns	PCD_A	I(0)0	12 bytes	Invalid CID: CID not sent while it should have been.	18 701 974 900 ns	1 047 800 ns	FDT PICC to PCD = 8.39 s	14443
18 858 017 600 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	18 858 300 800 ns	283 200 ns		14443
19 014 308 480 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	19 014 591 660 ns	283 180 ns		14443
19 172 068 980 ns	PCD_A	R(NAK)0	3 bytes	Invalid CID: CID not sent while it should have been.	19 172 352 160 ns	283 180 ns		14443
19 223 262 950 ns	PICC_A	I(0)0	5 bytes	Invalid CID: CID not sent while it should have been.	19 223 706 610 ns	443 660 ns	FDT PCD to PICC = 50.93 ms	14443

Conclusion

The delay caused by the relay attack depends on :

- The possibility for the tag to send S(WTX) requests.
- The Timeout used by the reader.
- The processing time on the tag.

Perspectives

- Since the value of the timeout depends on the value of the FWT, it is possible to extend the value of the timeout to 5s and thus the delay of the attack to approximately 5s also. This requires that:
  - We can choose the value of the ATS.
  - We can respect the time constraints during the initialisation and activation phases.

- Card simulation with Microprossx APIs.
- Relay attack on the Mifare Classic.
- Relay attack on the passeport.
- Mifare Plus : Getting start.

- Hancke : A practical Relay Attack on ISO 14443 Proximity cards.
- Kfir and Wool :Picking Virtual pockets using Relay Attacks on contactless Smartcard Systems.
- Francillon et al : Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.
- LibNfc documentation
- Microprossss Documentation.
- PCSC Windows documentation.
- ISO 14443 specification.