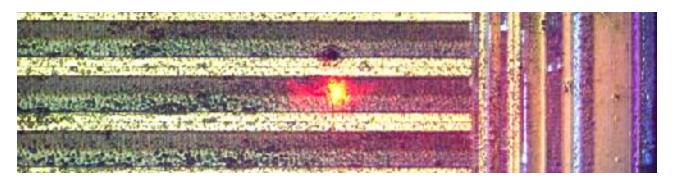


Practical optical fault injection on secure microcontrollers



Jasper G. J. van Woudenberg Marc F. Witteman Federico Menarini

FDTC2011, 28-9-2011

Public

This talk



- About...
- Contribution: develop specialized hardware to overcome previous higher order optical fault injection limitations
 - High fault injection repetition rate
 - Trigger synchronization to process
- Experiment 1: stable double-fault attack
- Experiment 2: pattern-based trigger synchronization
- Future: triple fault attacks, multi-location attacks
- Conclusion

Riscure Profile

- Founded in 2001 ٠
- Based in Delft, the Netherlands and San Mateo, ۲ California
- Clients in North America, Europe and Asia •
- **EMVco lab** accredited
 - Not a CC lab!
- Market leader in side channel test tools •
- Pay TV, smart card, mobile payment, smart metering •



3



Motivation



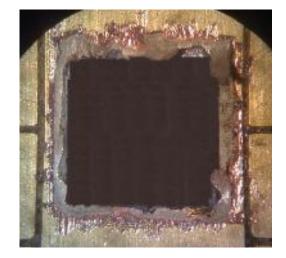
- Fault injection is the science (art?) of manipulating a device such that security mechanisms can be circumvented
- State-of-the-art smart cards come with FI Countermeasures
- Injecting faults multiple times can defeat those countermeasures
 - Mandatory requirement by EMVco and CC since 2011
 - Accurate control (timing, power) is very important
- Few publications of these attacks in practice using state-of-theart tools



Public

Experiments card 1

- Only main CPU, clocked externally at 1MHz
- Only countermeasure: double PIN verification
- Goal: skip both PIN verifications
- Approach:
 - Back side
 - Find sensitive location on chip
 - Find correct timing
- Show dual fault repeatability

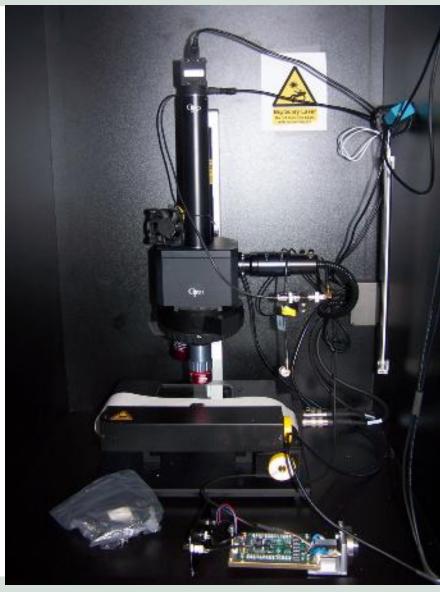




Optical setup used



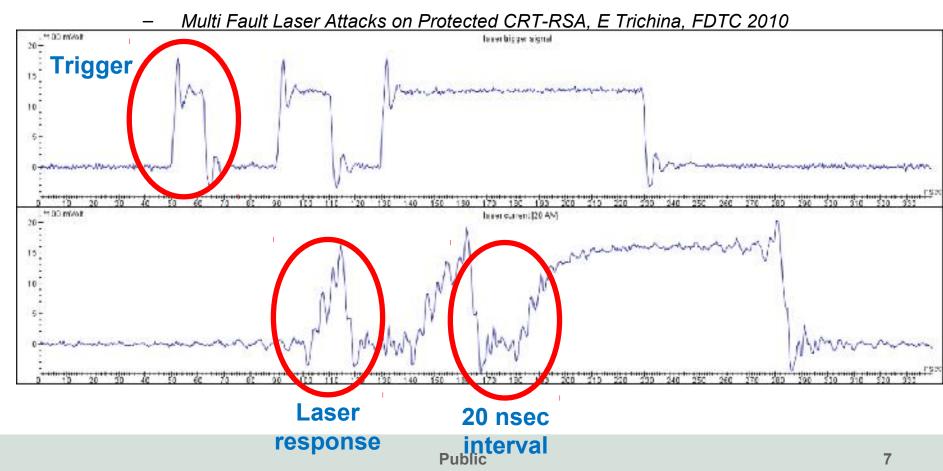
- Multimode diode lasers
 - 808nm: 14W
 - 1064nm: 20W
 - Pulse freq: 25 MHz ~ 40ns
 - 50ns trigger delay
- XY stage
- FPGA-based target control & trigger with 2ns time resolution
- FPGA-based real-time pattern matcher
- Oscilloscope
- Control software (Inspector)



Laser trigger response



- Diode lasers: constant delay, high repetition rate, arbitrary pulse length and power modulation
 - YAG: 200ms to recharge fully (can be shortened for less power)



Public

8

Attempt to inject faults during ATR communication ٠

- Scan over surface
- ATR sent by CPU: faults indicate CPU location •



Δ



B



Find timing



- Need to glitch two PIN verifications
- We cheat: card outputs which PIN verification succeeds
 - SW 6902: both fail
 - SW 6985: one succeeds, one fails
 - SW 9000: both succeed -> our goal
- Other feedback mechanisms used in 'blackbox' practice (e.g. power trace and/or timing)

Timing control

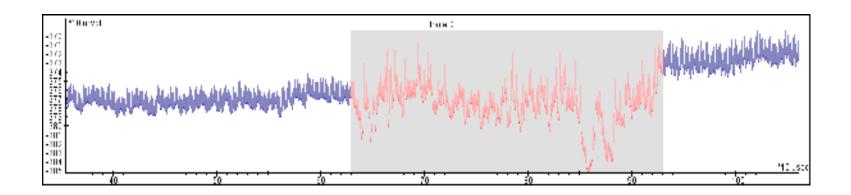


- Use FPGA to generate arbitrary triggers
 - At 2ns resolution
- **Program** in FPGA:
 - Send command
 - Wait x us (x s/w controlled)
 - Fire the laser
 - Wait y us (y s/w controlled)
 - Fire the laser
 - Receive answer

Timing 1



- Power trace to determine approximate timing
- Use one pulse between 630us and 930us
 - 1us increases: hit every instruction



Timing 1



00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00 00 00 00 00 F7 00 40 02 69 02 29 00 00 05 A0 1B 00 00

• Check output of card to find candidates for first timing

🛃 ve gu	tcher report	PIN pertur	bation modul	e (mulitple giffches) (started 2010/05/27/09:26:54)	100.00	00 00 0	0 F7 00 40) 02 69 02 29	00 00 0	15 AO 16	3 00 00	
Site level	diX		1	Eala	100.00	00.00.0	0 57 00 40	00240.02.20		E AO 11		
268	5017507	2502561		SKEZ 11 HE ST ST HE IS ST ST 75 ST 25 72 SS 54 0000 TS AT 14 00 10 TT RETURNED.	100.00	00.00.0	U F 7 UU 40) 02 69 02 29	00 00 0	O HU T	5 00 00	
	-11-20	Carsa.	-	and so the second s	00.00	<u></u>				E AO 11	<u>, oo oo</u>	
112	-77121-	0509504	-	AD FX TO FT THE ALL THE SAME TO 20 72 YE SAME OF AT LAND TO THE TO BE READ.	100.00	00.00.0	U F7 UU 40	02 69 02 29 02	000000	11 UH C	5 00 00	
325	-6-0160	4509564	-	2017/10/07/07/07/07/07/07/07/07/07/07/07/07/07						E 40.41		
10-	-525122	425095361	-	AD 17 YO 11 YO 10 YO 17 YO 17 YO 10 YO 17 YO 10 YO	100.00	00.00.0	U F7 UU 40) 02 69 02 29	000000	11 UH C	3 00 00	
111	-02075	0206201	-	AD FREE FITTE CALENT AT 52 19 70 10 20 72 10 50 0000 CE AT LO 00 10 CE DE CE 00 CE S						-		
265	10/0009	75075o1	-		1 UU UU I	00000	U F / UU 4U	02 69 02 29 0	, 00 00 0	15 AU 11	30000	
<i></i>	1199/80	35095o1	-	SREVICE HH SC ST HE TS SC 51, 73 53 /5 72 55 54 00 00 LS AC 14 00 00 LC BH CC 00 LC 1								
P1	1052956	2509561	-	SEE ALL HE SE ST HE TE SE SE AS 50 AS AC 55 SA 00 00 LE AL TA 00 10 LE BELL 00 LE L	1 UU UU I	UU UU U	U F / UU 4U) 02 69 02 29	,00,00,0	15 AU 18	3 00 00	
231 191	9000689) 37060-3	3509561	:	384711日日13日日1425.755767555540001541400011日日日								
200	3663796	0009001	-	2017 YO FT TO ALL TERN SK 15 75 TO 2017 YO TO 2000 TO 2011 YO TO 10 TO 2017 2017 YO FT TO ALL TERN SK 15 75 TO 2017 YO TO 2000 TO 2011 YO TO 2010 TO 2017 YO	1 OO OO I	00 00 0	0 F7 00 40	၂၉၃ နက္ က ၃၄	00 00 0	/5 AO 1/	3 00 00	
201	6001679	3005300	-	NOTE TO FEED ALL THAT SALES TO TO 20 TALES ADDOD TO AT LO DO NO TO FEED ADDOD TO AT AN								
-51	5070633	-30753300	-	20177 TO FT 1 (AL TEXT 52 15 7A 10 21 72 11 52 0000 TO AT 12 00 00 TO BE AT 00 12 5	100.00	00 00 0	0 F7 00 40	02 69 86 A	00 00 0	05 AO 1/	B 00 00	1
32-	57777000	-3607300	:	X0 EV CO FT CU 01 TE 40 52 CF 70 C0 70 72 C0 50 00 00 C0 00 10 00 00 C0 DF C0 00 C2 F								4
128	56325/0	383333	-	38 E / CE HHIEC 31 HE 16 50 ST / 35 SC / 5 40 SE 54 00 00 CE 40 14 00 00 CE 84 CE 00 CC .	1 AA AA I	00.00.0	0 F7 00 40	- J2 69 02 2 ¹	00 00 0	IS AN 17	3 00 00	
19 <u>0</u>	5509195	3633333	-	38E7112 FF 61 31 FE 16 50 51 73 53 76 70 55 54 00 00 16 A1 1A 00 10 11 BF 12 00 10 1			· · · · · · ·					
100 ·	538/17	303333	-	SBE7111 HH 51 ST HE 15 SC 51 75 5775 72 55 54 00 00 15 AU 14 00 10 11 BH 11 00 12 1	1 OO OO I	00.00.0	0 F7 00 40	- J2 69 02 2 ¹	00 00 0	<u>ΙS ΔΟ 17</u>	3 00 00	
212	5269700	3635,222	-	SBE712 HF 52 ST HE 15 S2 ST 75 S7 75 72 S5 S4 0000 15 AUTA 00.0012 BF 12 00 12		00 00 0				011011	0000	
77)	51-035-	-3062300	-	מסרבי המורח מנומים ביו ביני מממי לפירי איז ביו איז ביו איז	1 00 00	00.00.0	0 E7 00 40	D2 69 86 A	00 00 r	ስፍ ለብ 1/	B 00 00	1
329 	5017-307	306330	-	an 17 an 17 an 18 an 18 an 18 an 18 an 28 an 28 an 28 an 18 an 18 an 18 an 18 an 18 an	100.00	00 00 0		02 0 2 00 H	00 00 0		0 00 00	2
57 22-	-09-201	-30/653300	-	מסורה המשור המשור היותר ביותר המשור למינה לא היותר היותר היותר היותר היו	1.00.00	00.00.0	0 EZ 00 40	02 69 86 A	<u></u>	ስፍ ለብ 1/	B 00 00	8
100	-77121-	-3665300	-	20177 12 171 1 201 17 47 52 17 72 12 72 12 52 00 00 12 21 12 00 10 12 17 12 00 12 7 20177 22 17 22 21 17 12 13 52 22 72 22 72 72 22 54 00 00 22 42 14 00 20 22 07 22 00 22 7	100.00	00 00 0		JZ 07 00 M		po mo i		2
105	1525122	200,000	-	3867 CONTECTIVE REACTOR AND A CONTENT AND A	00.00	00.00.0	0 57 00 40	02 69 86 A	00.00.0		B 00 00	8
1			•			00.00.0	0 F / 00 4 0	JZ 09 00 M		ho wo t ⁱ	ם טט טנ	4
<					1.00.00	00.00.0		22.00.02.20		C AO 11	<u>, oo oo</u>	
witten.	dar				+ 00 00	00.00.0	0 F7 00 4(02 69 02 2 ⁴	00 00 0	O AU T	5 00 00	
					00.00	00.00.0	0 5 7 00 40		00.00			
					+ UU UU -	00.00.0	U F 7 UU 40	D2 69 86 A	00 00 (из но ц	B UU UL	4
										-		
					FUU UU F	<u>UU UU U</u>	U F 7 UU 40	02 69 86 A	00 00 0	05 AU 1,	B UU UL	4
												4
					100 00	00000	0 F7 00 40	D2 69 86 A	00 00 0	05 AO 1/	B 00 OC	4
												_
					100.00	00 00 0	0 F7 00 40	- 12 69 02 2 ⁴	00 00 0	/5 AO 1/	3 00 00	4





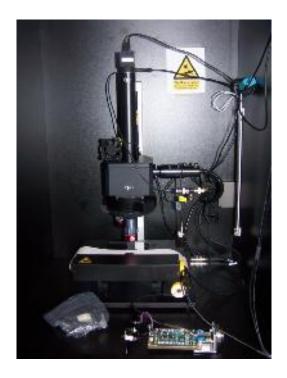
- Fix parameters for pulse 1
- Perform a second time interval scan for pulse 2

S VC Glitcher report - PIN perturbation mode	ule (multiple glitches) (started 2010-05-27-09:46:52)
l eta vilezzi en li elitari a indiali tra	
14 2 15 451 5 0	※E210年秋台市4552約約633526834000064414000000F7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
15 <u>2</u> 18 151 8 0	38 E7 10 〒 81 31 〒 +5 52 59 73 63 75 73 66 59 10 00 06 40 L4 00 10 00 8
.0 ≥ 10 4510 1 .7 ≥ 10 4510 1	2010 T 0.1 T 512 210 274 C 2 200 C 4 16 C 200 F7 00 00 0A 0A 3B E7 00 FF 81 31 FE 45 52 69 03 06 60 E0 00
17 2 12 451 a €a 1 0 2 12 451 a €a 1	
19 7 15 451 35 1	™************************************
AL 2 15 451 U SU L	*** 1+*** + ***************************
21 2 15 451 5 0	8 EV 10 + 60 C H 16 E 2 SV 16 C 16 2 E 10 10 E AU 16 (0, 10 10 B
20 0 15 451 5 1	※ED 日本1111日4559/2683526834 D00/64(14)0 D00時7 3B E7 00 FF 81 31 FE 45 52 69 73 63 75 72 65 5A
23 2 15 451 5 1 2- 2 12 4515 1	\$27.00 + \$1.00 + 5.00 (\$40.00 (\$40.000)
25 2 10 451 a Carl	
76 2 11 451 a start	
27 2 15 451 a. Stuff	
78 C 15 151 J 52 0	81/1 + 82/1 + 95/9 2014 2014 2014 100 4 100 100 7 00 40 2 69 86 At 00 00 05 A0 18 00 00 00 BE 00 00 03 00
20 2 15 451 50 0 30 2 15 451 50 0	
31 2 16 451 6 0	************************************
D2 2 10 4510 0	
CO 2 10 451 a ≪a 0	одоты, ткои техника роже и корол 7 00 40 <mark>2</mark> 2 69 86 AI 00 00 05 A0 1B 00 00 00 BE 00 00 03 00
F 2 F 4d a Kall	86/11/00/14/07/46/16/6/17/10/16/16/16/16/16/16/16/16/16/16/16/16/16/
St 7 15 451 452 11 St 7 15 451 2 11	
37 C 15 151 5 0	**************************************
38 2 15 151 5 0	※約 D 手約 2: 〒452 50 2542 55 22 43 50 00 05 40 14 00 10 008
30 2 16 451 5 0	※約つ手約10年41552901562551561950964614000006770040 2 90 00 D2 D0 00 05 A0 1B 00 00 00 BE 00 00 03 01
40 2 10 4510 0	
41 2 12 451 a -Ca 0 42 2 11 451 a -Ca 0	αστοποία τικαμέτα 1972 αρισσασκαί και σομή 7 00 40 2 90 00 D2 D0 00 05 A0 1B 00 00 00 BE 00 00 03 01
48 2 15 451 a - 550 0	812 1 + 812 + 852 M 2 m 2 M 2 m 2 m 2 m 2 m 7 00 40 2 90 00 D2 D0 00 05 A0 1B 00 00 00 BE 00 00 03 01
16 C 15 15 5 0 0	81/ TH 812 H GRAVING ON A CHINE A TABLET THE CONTRACTOR C
15 2 15 451 J. S. I	######################################
16 C 15 -151 5 1	38 E7 1D 平 81 22 元 45 52 59 72 63 75 72 63 64 10 00 05 40 14 00 10 00 B
<	00 00 05 A0 1B 00 00 00 BE 00 00 03 00 00 00 A0 1B 00 00 00 BE 00 00 03 00 5
nga tanàn ao amin'ny faritr'o amin'ny fari	

Conclusions card 1



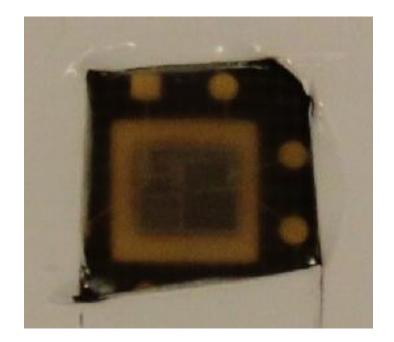
- 1000/1000 injections successful
- Delay between pulse 1 and 2 is 33us
- Changing timing by **1us** changes outcome
- 808nm laser does not work, 1064nm laser does
- Repeatability requires fast and jitterfree system
- Diode lasers + fast control fit for this purpose



Experiments card 2



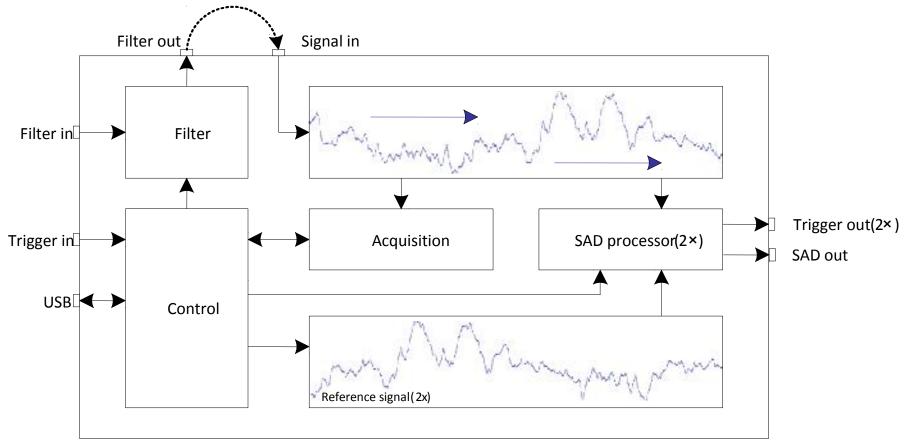
- Main CPU + crypto accelerator, clocked internally ~30MHz
- Countermeasure: unstable clock, FI detection & card termination
- Goal: corrupt DES output, keep card alive
- Approach:
 - Front side (through epoxy!)
 - Create synchronized trigger
 - Find sensitive location on chip
- Show synchronization
- Show termination prevention



Create synchronized trigger



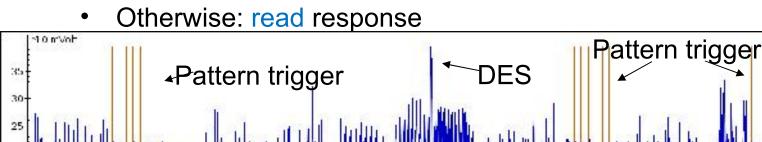
- Use real-time (filtered) pattern matching
- FPGA based, A/D running at 100MHz

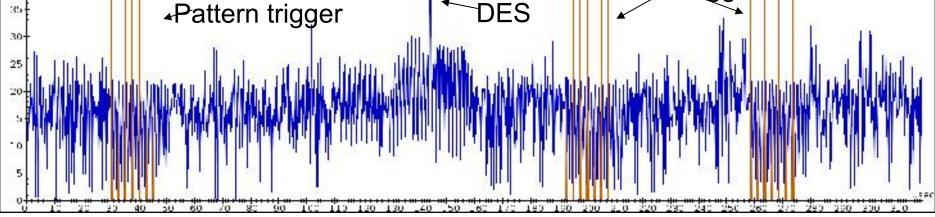


FI control (FPGA)



- Send command
- Wait for external trigger
- Wait x us (x software controlled)
- Fire the laser ۲
- If no external trigger within 100us: power off card ۲





Finding the location

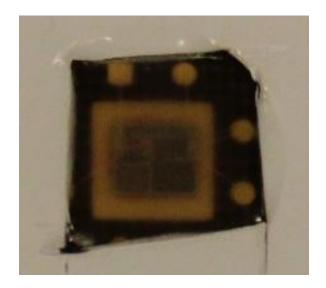


- Countercountermeasure in place: safe to scan surface
- Found timing where DES accelerator was producing faulty outputs
- Repeatly fire here (>50% success rate)

Conclusions card 2



- Before: wildly varying results, card termination <1000 injections
- After:
 - often DES output == DES input (break protocols)
 - card still happy at 60000 injections
- Timing jitter can be countered by:
 - pattern based triggering
 - a stable and fast laser response
- Card termination can be countered by:
 - pattern based triggering
 - control response <100us



Latest development: triple glitch

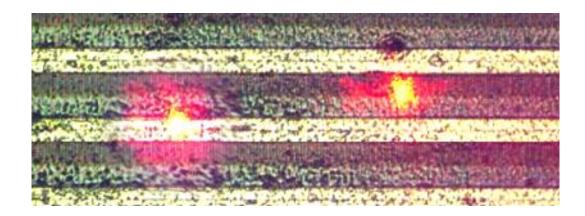


- Performed successful triple glitching
 - RSA-CRT: glitch CRT + double verification
 - Latest smart card technology
 - 1% success rate (of obtaining full private key)
 - Lab condition: able to control countermeasures; no card termination

Latest development: multi location



- Add fiber-guided laser to setup
- Add second XY manipulator
- Double laser trigger
- Challenge: finding the (right location/time/etc)²...



Summary



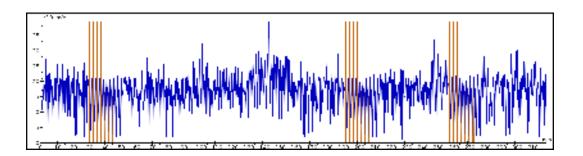
- State-of-the-art optical fault injection equipment allows much more control
 - Overcome limitations imposed by non-diode lasers (YAG,DPSS)
 - Overcome fixed-delay trigger limitations
- Precisely inject arbitrary number of faults
 - Experimentally: success with up to three



Conclusion



- EMVco and CC moved to multi-time and will likely move to multilocation FI
- Countermeasures need to be improved
 - Double verification not sufficient anymore
 - Side channel patterns (also after filtering!) should be minimized



Discussion



Jasper van Woudenberg Senior Security Analyst vanwoudenberg@riscure.com Riscure B.V. Frontier Building Delftechpark 49 2628 XJ Delft The Netherlands

Phone: +31 (0)15 251 4090 www.riscure.com

Shameful plug: WE ARE HIRING!

