FAME: Fault-attack aware Microprocessor

PIs: Patrick Schaumont, Leyla Nazhandali
{schaum,Leyla}@vt.edu http://rijndael.ece.vt.edu/fame


Why are Faults a Security Issue?

- May cause information leakage of secrets

```
if (key_bit)
   r1 = r1 + 1;
else
   r0 = r0 + 1;

out = f(r1);
```

fault in `r1`

`key_bit` *leaks indirectly via* `out`

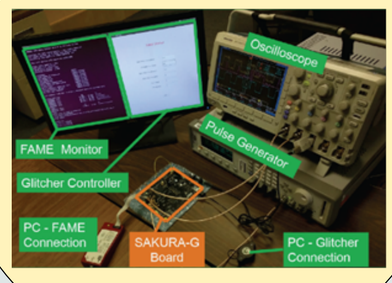
- May enable external control of execution
  - Denial of service
  - Control of critical decisions

```
if (! access_allowed )
   abort( );
```

instruction_skip

Fault Injection Tools of the Trade

Clock Glitches

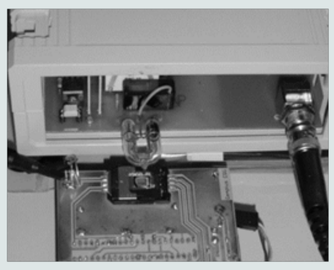


[Yuce 2016]

Laser

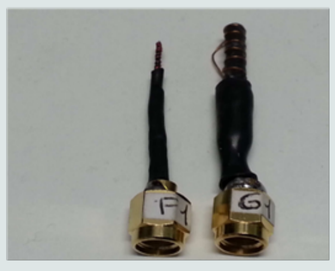
[Selmke 2016]

Light Pulses



[Bar-El 2004]

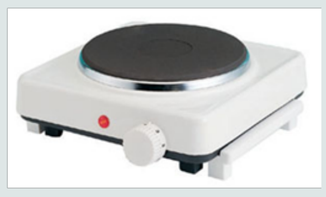
EM Pulses



[Zussa 2014]

Voltage Starving

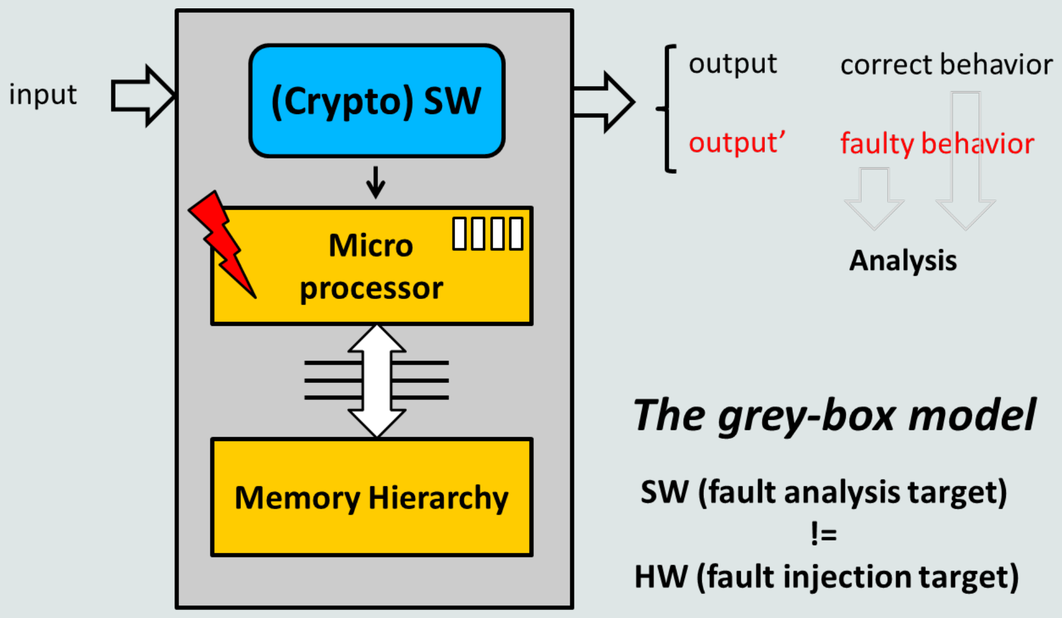
Temp Hike



focus in this project

Attacks

Micro-architecture Aware Fault Injection



The grey-box model

SW (fault analysis target)
!=
HW (fault injection target)

Example: Fault attack for a 7-stage pipeline

```
ld      [%o3 + 0xb0], %o4
ldub    [%o0 + 0xb], %o5
ldub    [%o4 + 0xb], %g1
xor     %g1, %o5, %g1
stb     %g1, [%o3 + 0xb]
```

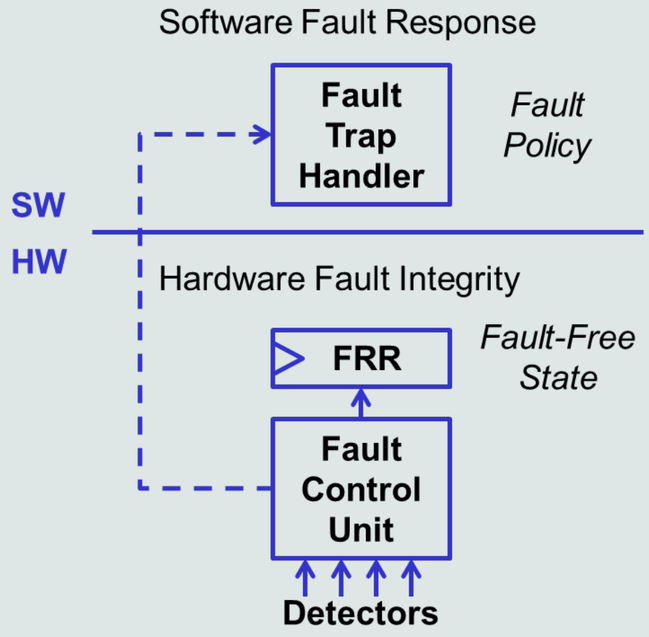
F	D	A	E	M	X	W
LD1						
LD2	LD1					
LD3	LD2	LD1				
XOR	LD3	LD2	LD1			
ST	XOR	LD3	LD2	LD1		
			LD3	LD2	LD1	
	ST	XOR		LD3	LD2	LD1
		ST	XOR		LD3	LD2
			ST	XOR		LD3
				ST	XOR	

Result:

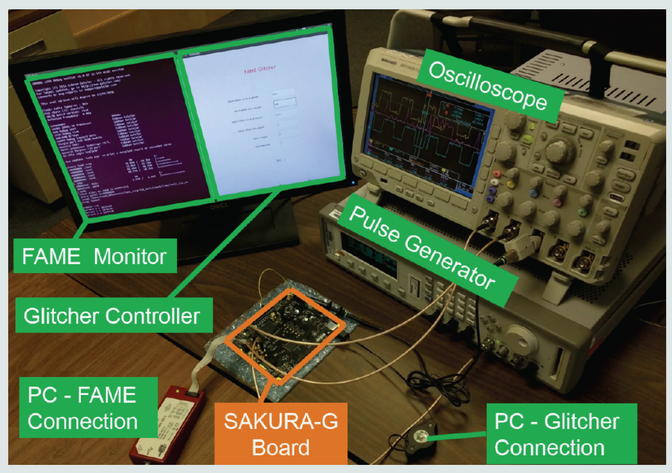
- 11 times less fault injections needed;
- Broken software countermeasures

Countermeasures

Micro-architecture Fault Response



Example: Prototype Setup



Result:

- Prototype LEON3 on FPGA;
- ASIC Tape-out

Interested in meeting the PIs? Attach post-it note below!

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

National Science Foundation
WHERE DISCOVERIES BEGIN

Semiconductor Research Corporation