Fault attack on the communication architecture of a RISC-V based system

Hongwei ZHAO, Vianney LAPÔTRE, Guy GOGNIAT

Lab-STICC, UMR 6285, Université Bretagne Sud, Lorient, France - firstname.lastname@univ-ubs.fr

Abstract

Fault attacks aim to disturb integrated circuits using methods such as power spikes [1], clock glitches [2] or electromagnetic injection [3] to break security system or steal information. A SoC is made up of numerous IPs which are connected to each other by a communication architecture. Our work focuses on the wishbone [4] bus architecture of a RISC-V based system obtained using the LiteX framework. Vulnerabilities are identified through fault injection simulations and possible attack vectors are highlighted.

Vulnerabilities within the communication architecture

Figure 1 illustrates a simplified SoC communication architecture with different components. Data, address, and control signals are transferred through a bus. Listing 1 is the program under attack, attack target is highlighted in red as in the SoC architecture.

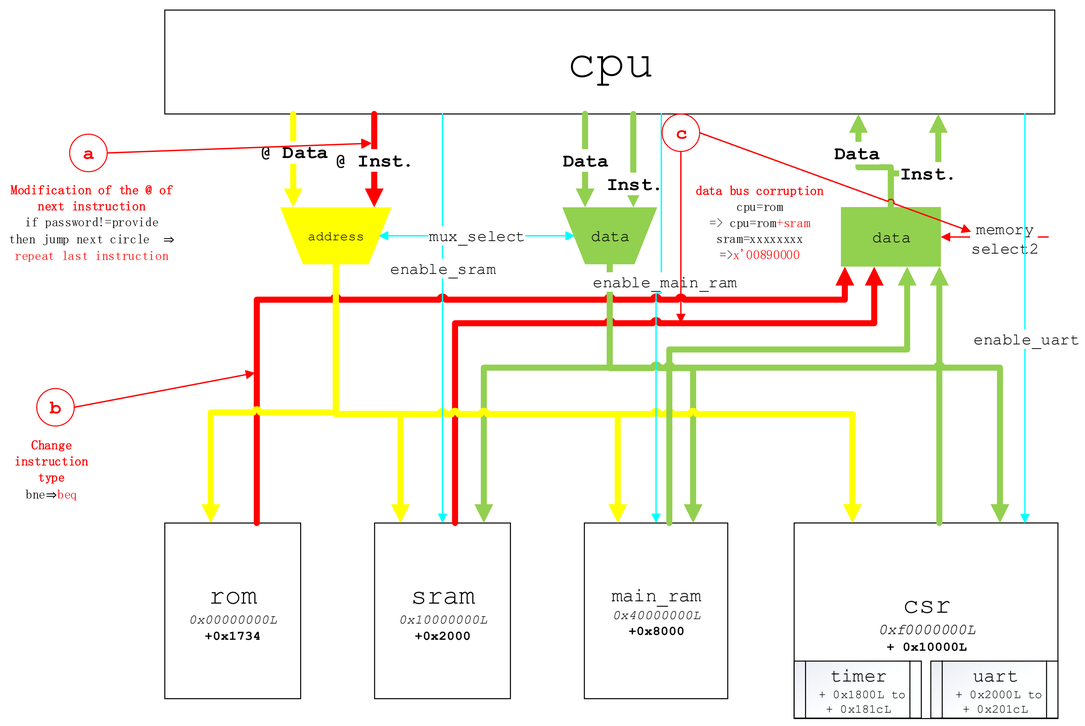

Figure 1. Fault propagation paths in the communication architecture

```
int main(void)
{
   ...
  password=256;
  provide=334;
  for (try_left=3; try_left>0; try_left--) {
  if (password==provide) {
          try_left=3;
          printf("good key\n");
          return 0;
        }
  else printf("remain %d tries\n", try_left-1);
  }
   ...
}
```

Listing 1. Attack targets in a C code

Fault attacks scenarios

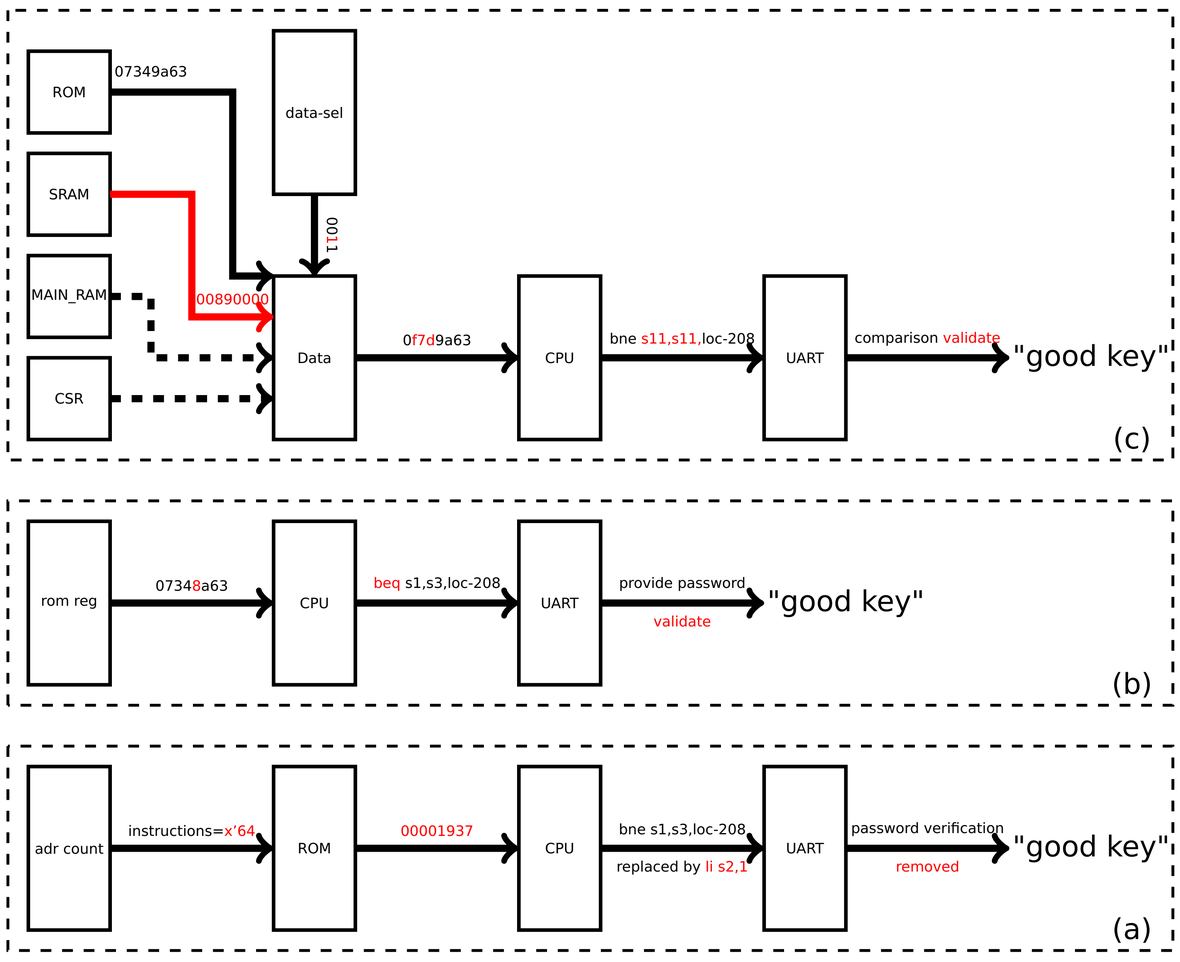

Figure 2. Fault propagation in the communication architecture

Figure 2 shows fault propagations corresponding to threats in figure 1. Table 1 evaluates these attacks before. From above to below, they correspond to (c) (b) (a) in Figure 2.

Fault injection senario	Target of the fault	Fault type	Complexity of the attack
corrupt data bus (c)	SRAM and control signal in register	1 bit_flip in register	average (need a write in SRAM)
change instruction type (b)	data bus input	1 bit_flip in register	low
change instruction order (a)	address bus input	1 bit_flip in register	low

Table 1. Evaluation of fault attacks

Conclusion and future work

Communication architecture can be a target of fault injection attacks. Several vulnerabilities have been identified and illustrated. Future work aims to generalize fault injections in the communication architecture and to propose countermeasures.

Bibliography

1. C. Aumüller et al, "Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures", CHES, 2002, pp. 260–275.
2. S. Endo et al, "An on-chip glitchy clock generator for testing fault injection attacks", J. Cryptograph. Eng., Dec. 2011, pp. 265–270.
3. P. Maistri et al, "Electromagnetic analysis and fault injection onto secure circuits", VLSI-SoC, 2014, pp. 1-6.
4. R. Herveille et al, "Wishbone B4", OpenCores Organization, 2010.