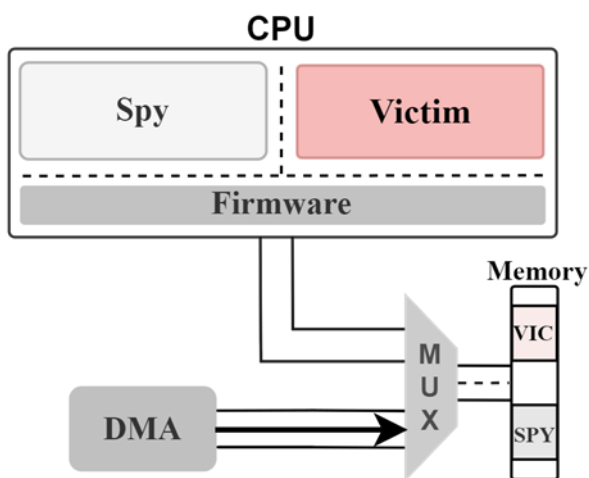



# Attack Overview – Toy Example



```
cmp    r3, #0                1 clk
beq.n  ELSE                  3 clk (else), 1 clk (if)
IF:    movs    r3, #1        1 clk
      str     r3, [r7, #0]   1 clk
      b.n     r3, #0         2 clk
ELSE:  mov     r3, #0        1 clk
      str     r3, [r7, #0]   1 clk
END:   nop                     1 clk
```

```
if(s==1)
    var=1;
else
    var=0;
```

SECRET = 1



Clock	t	t+1	t+2	t+3	t+4	t+5	t+6
If	cmp	beq	movs	str	b	b	nop
Trace	---	---	---	X	---	---	---
Else	cmp	beq	beq	beq	movs	str	nop
Trace	---	---	---	---	---	X	---