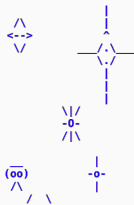


Logic-monsters: Ataques de supply-chain a nivel de silicio



Full Stack Tech 2017

Alfredo Ortega

2 de diciembre de 2017


Table of contents

1. Introducción
2. Compuertas lógicas
3. Techlibs
4. Ataques/Seguridad
5. Conclusion

Introducción

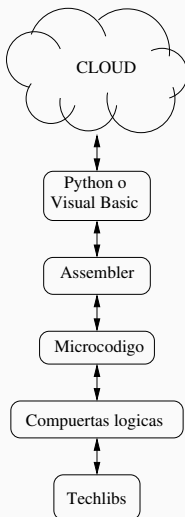


Figura 1: No hagan esto en su casa.

- Técnico electrónico
- Doctor en Informática ITBA
- Investigador en seguridad informática
- > **4000 followers** en Twitter  @ortegaalfredo

Introducción: Stack

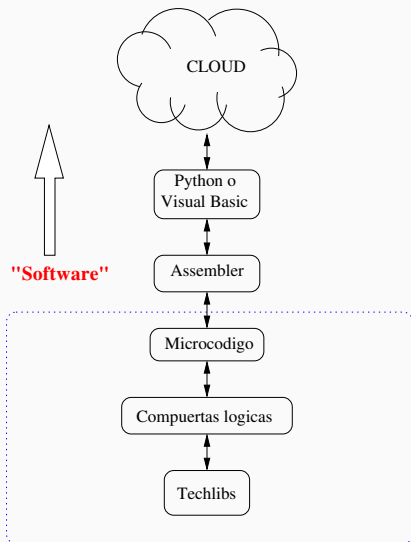
Software Stack:



- **Microcódigo:** Verdaderas instrucciones del CPU
- **Compuertas lógicas:** Ejecutan microcódigo
- **Techlibs:** Spec de compuertas. Ej. TSMC 90nm, IBM 14nm, Etc.

Introducción: Stack

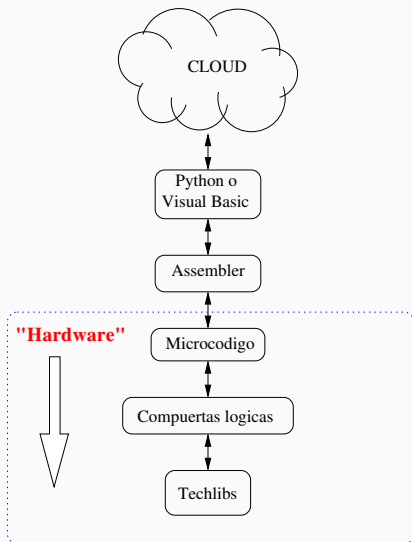
Software Stack:



- **Microcódigo:** Verdaderas instrucciones del CPU
- **Compuertas lógicas:** Ejecutan microcódigo
- **Techlibs:** Spec de compuertas. Ej. TSMC 90nm, IBM 14nm, Etc.

Introducción: Stack

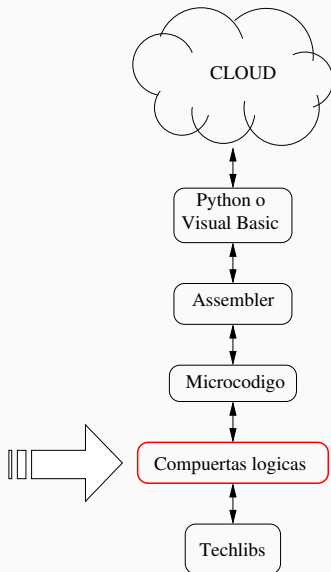
Software Stack:



- **Microcódigo:** Verdaderas instrucciones del CPU
- **Compuertas lógicas:** Ejecutan microcódigo
- **Techlibs:** Spec de compuertas. Ej. TSMC 90nm, IBM 14nm, Etc.

Compuertas lógicas

Compuertas: nivel



Compuertas: HDL

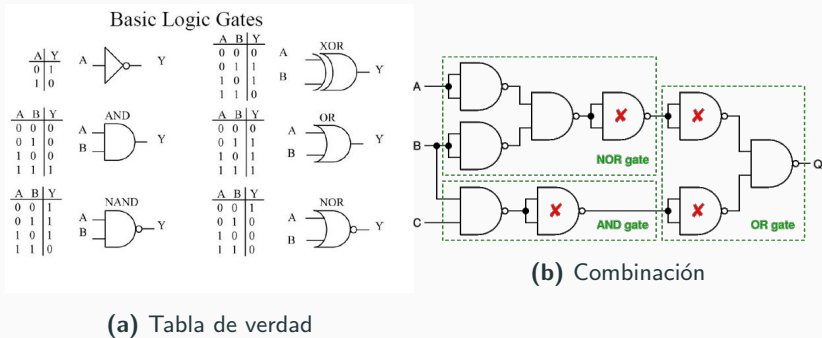
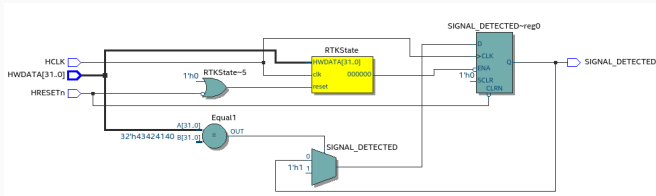


Figura 2: Compuertas básicas

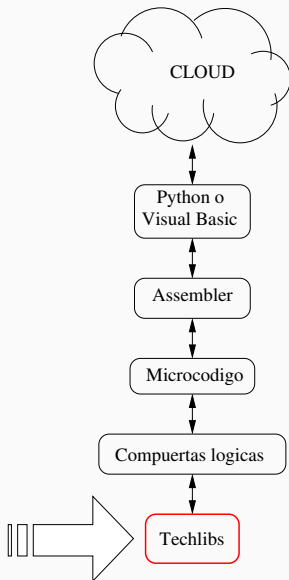
Compuertas: HDL



```
1  always @(posedge HCLK or negedge HRESETn)
2      begin
3          if (!HRESETn) // Reset
4              begin
5                  RTKState<='RTK_FIND.START;
6                  SIGNAL_DETECTED<=0;
7              end
8          else begin
9              case (RTKState)
10                 'RTK_FIND.START: // Find first part of cookie
11                     if ( HWDATA == 'RTK_COOKIE.1)
12                         begin
13                             RTKState<='RTK_FIND_2;
14                         end
15                 endcase
16             end
17         end
```

Listing 1: Verilog, ejemplo.

Techlibs



Como se hace una compuerta?

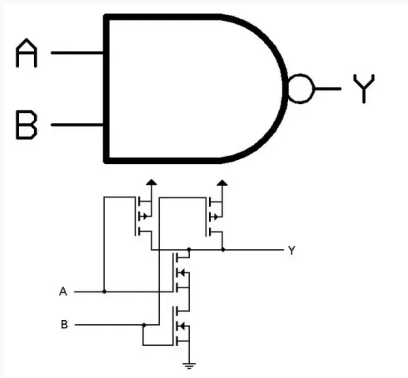


Figura 3: Nand: Diagrama CMOS

Como se hace una compuerta?

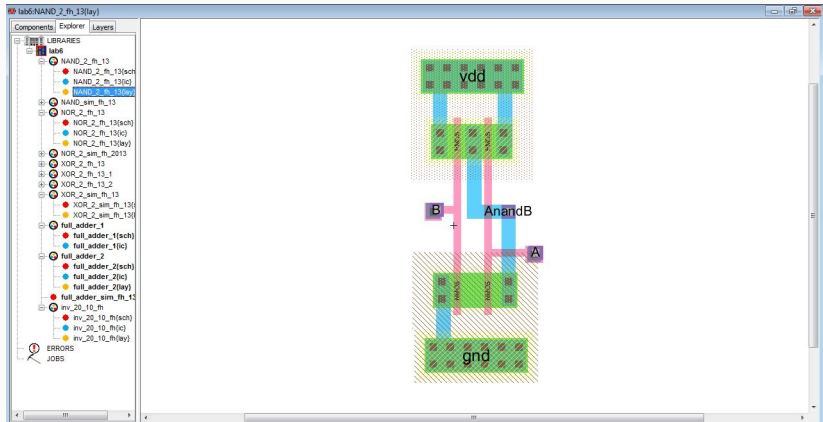


Figura 4: Nand: Diseño digital

Como se hace una compuerta?

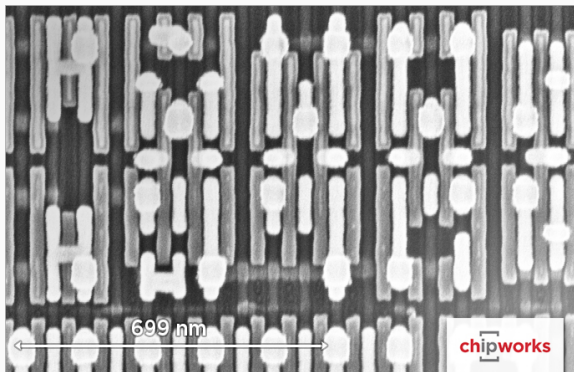


Figura 5: Nand: Microscopio (14nm Intel)

Como se hace una compuerta?

```

1  MACRO NAND2X1
    CLASS CORE ;
3  FOREIGN NAND2X1 0.000 0.000 ;
    ORIGIN 0.000 0.000 ;
5  SIZE 3.600 BY 15.000 ;
    SYMMETRY X Y ;
7  SITE core ;
    PIN A
9      DIRECTION INPUT ;
        PORT
11         LAYER metal1 ;
            RECT 0.300 4.350 0.900 5.550 ;
13     END
    END A
15    PIN B
        DIRECTION INPUT ;
17        PORT
            LAYER metal1 ;
19            RECT 2.700 7.950 3.300 9.150 ;
                END
21    END B
    PIN gnd
23        DIRECTION INOUT ;
        USE GROUND ;
25        SHAPE ABUTMENT ;
        PORT
27            LAYER metal1 ;
                ...
29    END gnd
END NAND2X1

```

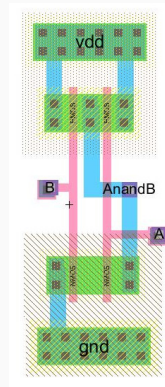


Figura 6: Nand: Macro Techlib osu025 (250nm)

Ataques/Seguridad



- Simple modificacion del código fuente
- Ej. Backdoors genéricos (portables)
- Debilitación de criptografía.

Demos!

Logic Monsters project

Logic Monsters - Chromium


Logic Monsters x


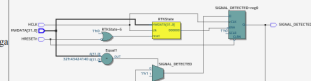
Secure | <https://ortegaalfredo.github.io/logic-monsters/>

Apps Unable to switch messages: unre... pr yComp - VCG vie w Siding Spring Su ALBERICK - Com

Logic Monsters

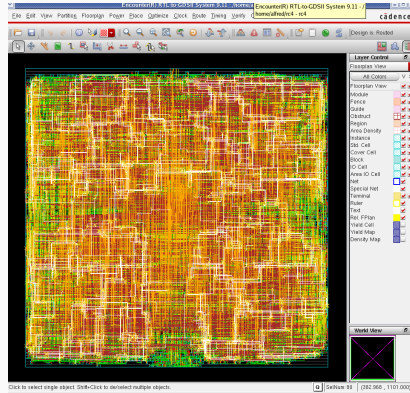
A collection of malicious logic, AKA shellcode for hardware



Name	Description	Size	Author	Preview
Malproxy	Small hardware that fits between the bus master (usually the CPU) and a slave I.E. an ARM processor and the memory. When the logic see a 56-bit cookie (32 bits+24 bits) it reads a command, data and proceeds to disconnect the CPU and execute the command over the main memory (command can be read/write memory). This allows to embed malicious data in any bus transfer that can be interpreted by this logic outside control of the main CPU. This works mainly on ARM processors as it is compatible with the AHB LITE bus.	Total logic elements: ~140 (Cyclone IV) Total registers: ~90 (Cyclone IV)	aortega	
Sorath	Tiny state-machine that recognizes a 64-bit magic number in a 32-bit bus and activates a flag. When the logic see the cookie (32 bits+32 bits) it enables a single-bit register. This can be attached to a privilege register, so it elevates privileges when the magic-number is seen. "The mystery of Sorath and his number 666 holds the secret of black magic."	Total logic elements: ~17 (Cyclone IV) Total registers: ~2 (Cyclone IV)	aortega	

Conclusion

Conclusion



- Hay muchas más capas en el stack.
- Todas se especifican con archivos de texto.
- Todas pueden tener problemas de seguridad.

References I

Source: <https://ortegaalfredo.github.io/logic-monsters/>

Thank you!

