SoC Security: Architecture, IP, or CAD?

Professor Ryan Kastner

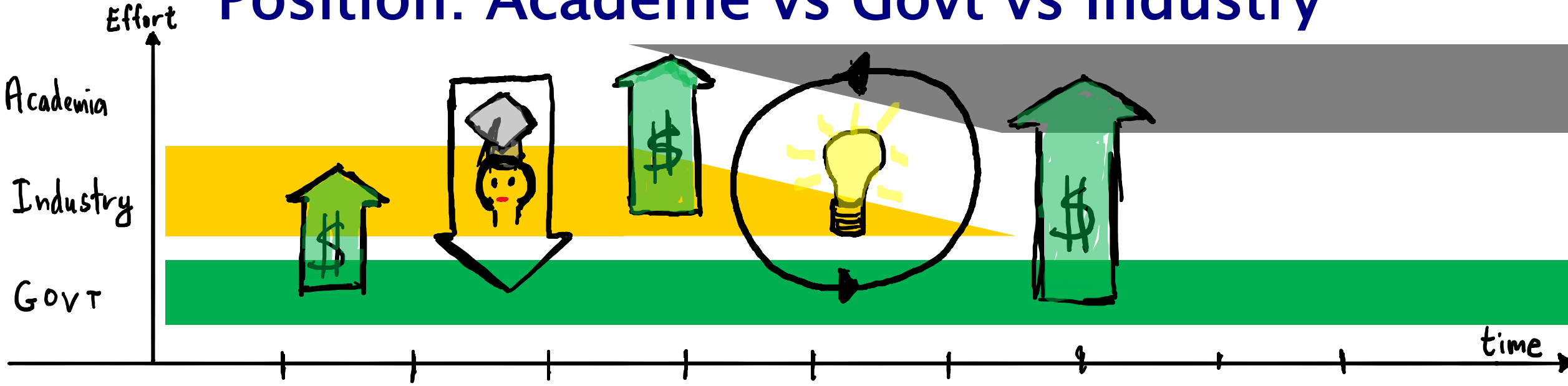
Dept. of Computer Science and Engineering

UC San Diego

kastner@ucsd.edu

http://kastner.ucsd.edu

Position: Academe vs Govt vs Industry



Position: IP Security is (mostly) solved

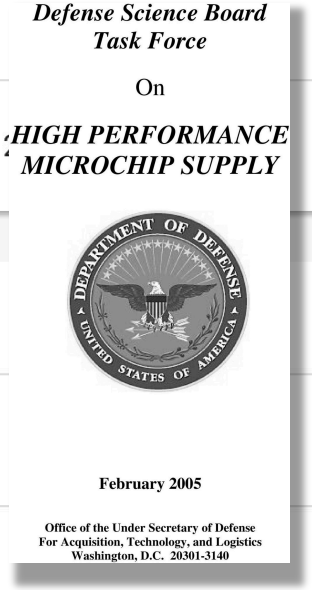
Google Trends | Explore

hardware trojan
Search term

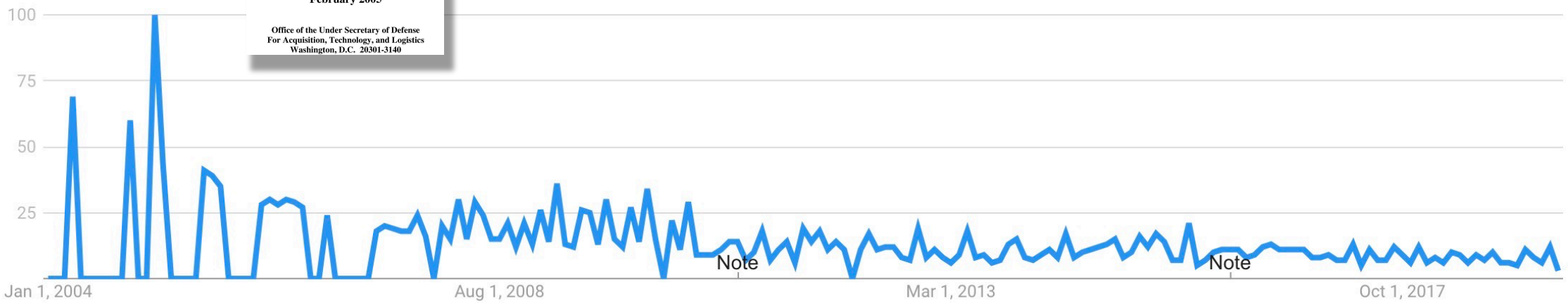
+ Compare

United States | All categories | Web Search

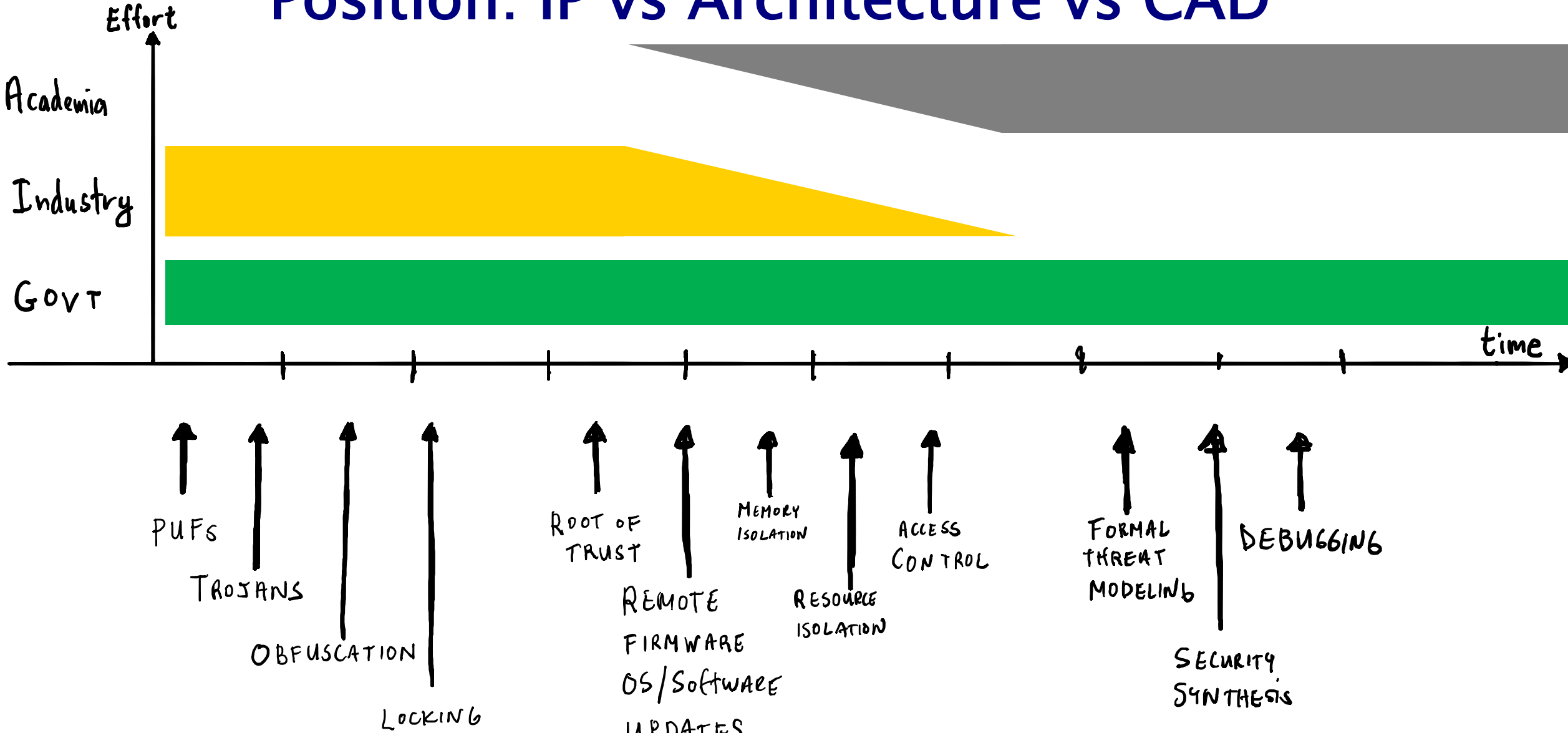
Interest over time



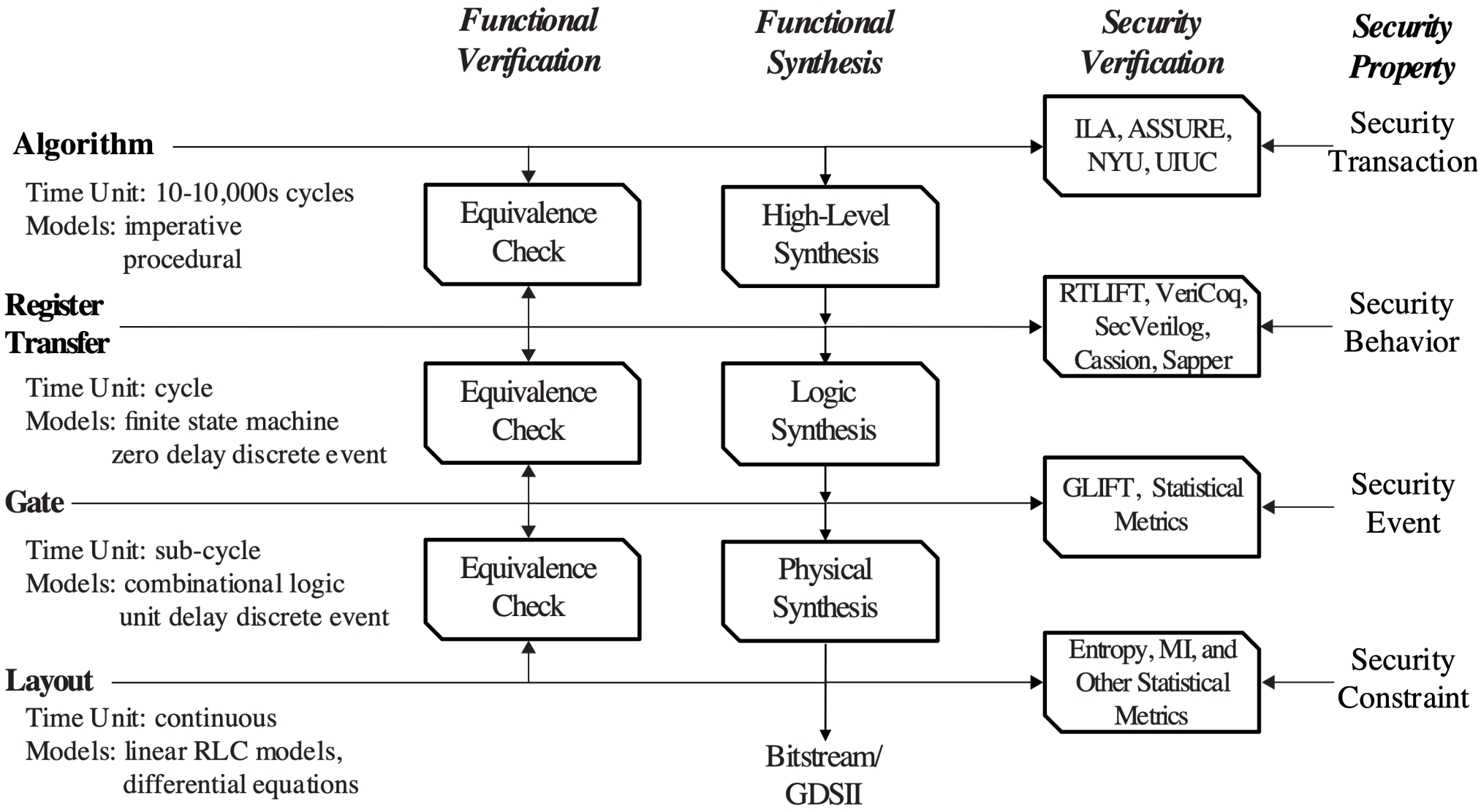
PUFs, Obfuscation, Locking, ...



Position: IP vs Architecture vs CAD



Pressing Need: Formal Threat Models



Wei Hu, Alric Althoff, Armaiti Ardeshiricham, and Ryan Kastner, "**Towards Property Driven Hardware Security**", *Microprocessor Test and Verification Conference*, December 2016 (pdf)

Pressing Needs/Challenges: Security Debugging

1) Write HW, SW, FW/, …

```
input in;
output out;
output [7:0] counter;

reg [7:0] counter;

wire counter_overflow = (counter == 8'hff);
wire counter_underflow = (counter == 8'h00);

always @(posedge clk or negedge xreset)
begin
        if (xreset == 0)
                counter <= 0;
        else if (en && in && !counter_overflow)
                counter <= counter + 1;
        else if (en && !in && !counter_underflow)
                counter <= counter - 1;
        else
                counter <= counter;
end
```

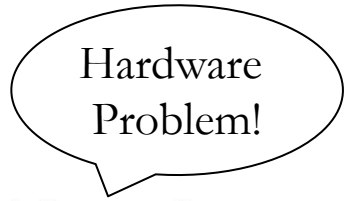
2) Write Security Properties

```
assert isolation(request[0],request[1])
assert …
```

3)

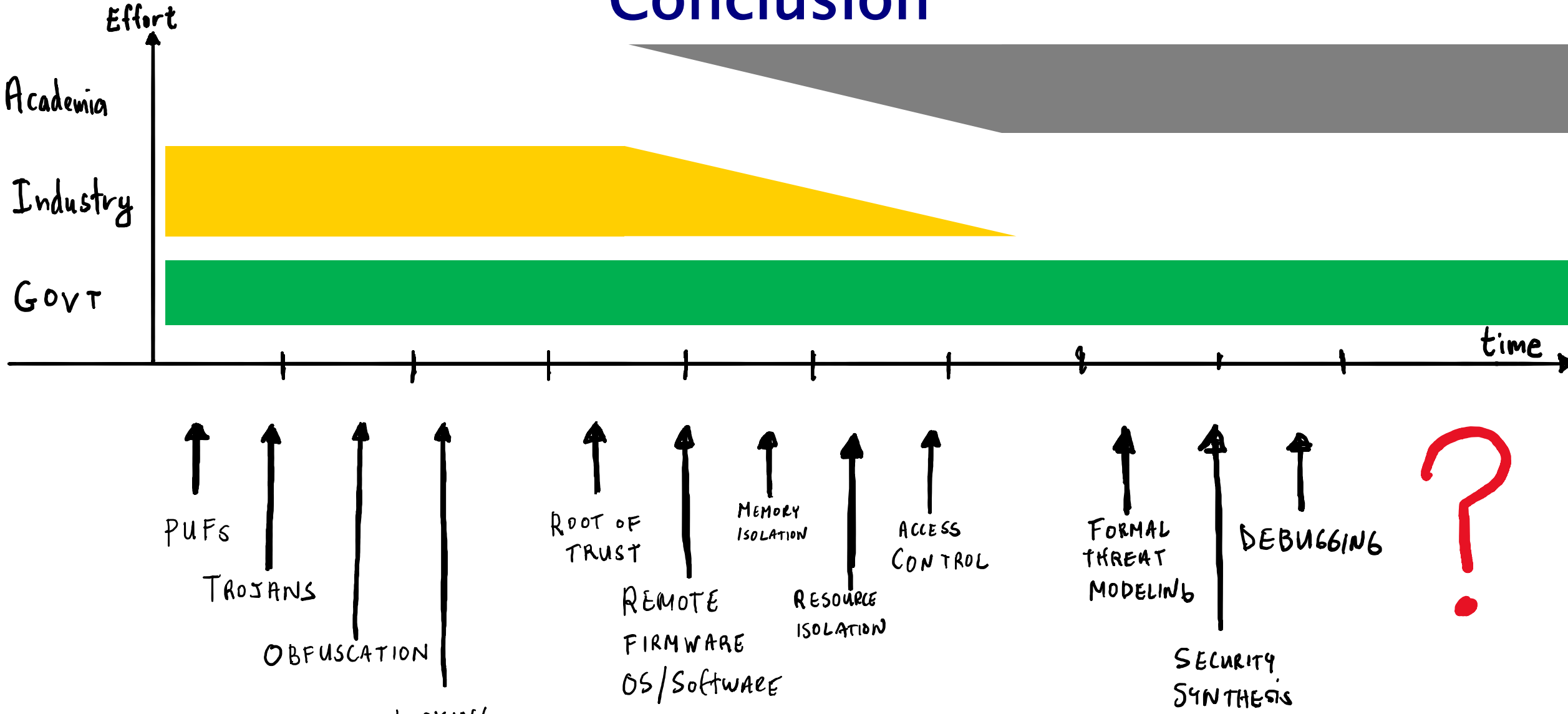
4) Fix security flaws

- Security Experts ¯_(ツ)_/¯



- Hardware Designers ¯_(ツ)_/¯

Conclusion


Effort
Academia
Industry
Govt
time
PUFs
TROJANS
OBFUSCATION
LOCKING
ROOT OF TRUST
REMOTE FIRMWARE OS/Software UPDATES
MEMORY ISOLATION
RESOURCE ISOLATION
ACCESS CONTROL
FORMAL THREAT MODELING
SECURITY SYNTHESIS
DEBUGGING
?
IP
ARCHITECTURE
EDA