JTAG Enum

a power-analysis hunt

- rick@riverloopsecurity.com
Breakthrough silicon scanning discovers backdoor in military chip

Sergei Skorobogatov\textsuperscript{1} and Christopher Woods\textsuperscript{2}

\textsuperscript{1} University of Cambridge, Computer Laboratory, Cambridge, UK  
  sps32@cam.ac.uk
\textsuperscript{2} Quo Vadis Labs, London, UK  
  chris@quovadislabs.com
Magic Command in

Unencrypted firmware out
- Read memory
- Step through instructions
- Interact with peripherals
- Breakpoints
- Etc.
Test Access Port (TAP)

- TDI
- TCK
- TRST
- TMS

- Instruction Register
- ID Register
- Data Register

MUX

TDO
Instruction Shifted In

Test Access Port Controller (TAP)

TDI

TCK

TMS

TRST

Instruction Register

ID Register

Data Register

MUX

TDO
Data Shifted Out

Test Access Port Controller (TAP)

- TDI
- TCK
- TMS
- TRST
- Instruction Register
- ID Register
- Data Register
- MUX
- TDO
Data Register can be of arbitrary length

Instruction can be carried out during the DR shift out
Data Register can be of arbitrary length

Instruction can be carried out during the DR shift out

Check length of data register

Check if anything happened
Test Access Port Controller (TAP)

- **TCK**
- **TMS**
- **TRST**

**Instruction Register**

- **TDI**
- **TDO**

**ID Register**

- Check length of data register
- Check if anything happened

**Data Register**

- Data Register can be of arbitrary length
- Instruction can be carried out during the DR shift out

**POWER ANALYSIS**
did anything happen?
Trace 1  
1 1 2 3 5 8 13 1 1 2 3 5 8 13

Trace 2  
0 1 1 2 3 5 8 13 1 1 2 3 5 8

Averaged Trace  
0.5 1 1.5 2.5 4 6.5 10.5 7.5 1 0.5 2.5 4 5 10.5

Muted Features
Two out-of-phase signals can mute features
Sum of Absolute Differences

\[ SAD(x, y, u, v) = \sum_{dx=-W}^{W} \sum_{dy=-W}^{W} |I_c(x+dx, y+dy) - I_r(x+u+dx, y+v+dy)| \]
Sum of Absolute Differences

\[ SAD(x, y, u, v) = \sum_{dx=-W}^{W} \sum_{dy=-W}^{W} |I_c(x+dx, y+dy) - I_r(x+u+dx, y+v+dy)| \]

Trace 1

\[ 1 1 2 3 5 8 13 1 1 2 3 5 8 13 \]

Trace 2

\[ 0 1 1 2 3 5 8 13 1 1 2 3 5 8 \]

Subtract & absolute

\[ 1 0 1 1 2 3 5 12 0 1 1 2 3 5 \]

SUM = 37
Sum of Absolute Differences

Trace 1

\[ \begin{array}{cccccccccc}
1 & 1 & 2 & 3 & 5 & 8 & 13 & 1 & 1 & 2 & 3 & 5 & 8 & 13 \\
\end{array} \]

Trace 2

\[ \begin{array}{cccccccccc}
0 & 1 & 1 & 2 & 3 & 5 & 8 & 13 & 1 & 1 & 2 & 3 & 5 & 8 \\
\end{array} \]

Subtract & absolute

\[ \begin{array}{cccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array} \]

\[ \text{SUM} = 0 \]
Sum of Absolute Differences

1. Repeat N times in your window
2. Select Trace with the minimum sum

SUM = 0
Results on STM32F
TL;DR:
• Specialty in low-level embedded: HW/FW/RF
• HW assessment/pen-testing
• Binary analysis on firmware
• Cryptographic design & review
• RF reverse engineering