Analysis of Data-Leak Hardware Trojans In AES Cryptographic Circuits

Trey Reece, William H. Robinson

Department of Electrical Engineering and Computer Science
Security and Fault-Tolerance Group
Vanderbilt University

October 9, 2013

Brief Overview

This study explored the impact of 18 Trojans:

- All Trojans leaked sensitive information
- All Trojans were implemented on the same circuit

The Trojans explored in this study were found to have:

- Very small footprints
- No fixed cost
  - Widely varies even for similar Trojans
- A cost dependent upon designer, not Trojan

"The concept of trust requires an accepted dependence or reliance upon another component or system" [1]

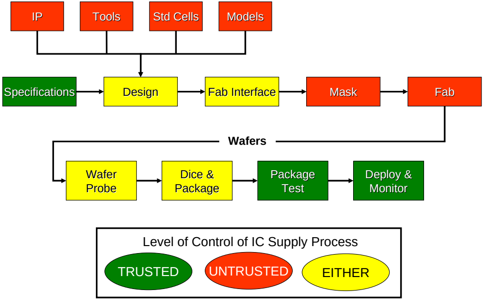


Figure (1). How trusted are steps in circuit production?[2]

[1] C. E. Irvine and K. Levitt, "Trusted hardware: Can it be trustworthy?" in *44th ACM/IEEE Design Automation Conference (DAC '07)*, 2007, pp. 1–4

[2] D. Collins, "DARPA Trust in IC's Effort (BRIEFING CHARTS)," 2007

Can we trust Fabrication Plants?

Table (1). 2011 Top-10 Semiconductor Foundries [3]

Rank	Foundry	Location	Sales (USD)
1	TSMC	Taiwan	14,600M
2	UMC	Taiwan	3,760M
3	GlobalFoundries	U.S.	3,580M
4	Samsung	South Korea	1,975M
5	SMIC	China	1,315M
6	TowerJazz	Israel	610M
7	Vanguard	Taiwan	519M
8	Dongbu	South Korea	500M
9	IBM	U.S.	445M
10	MagnaChip	South Korea	350M

[3] Semiconductor and Manufacturing Design Community, http://semimd.com/blog/2012/02/10/umc-seeks-to-shed-image-as-'fast-follower'/

Hardware Trojans

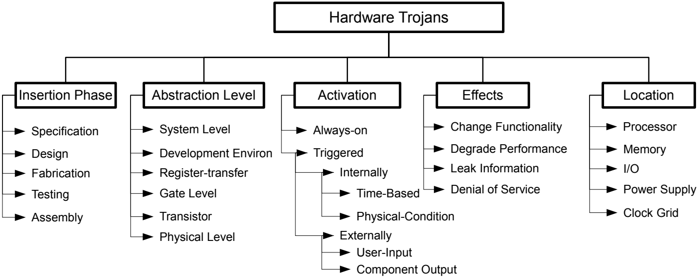


Figure (2). Sample Hardware Trojan Taxonomy[4]

There are many possible ways to maliciously influence a circuit

[4] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, pp. 39–46, 2010

Finding a Solution

How to mitigate Trojans inserted during fabrication:

- Prevent Trojan insertion
  - Circuit Hardening
  - Circuit Obfuscation
- Secure the fabrication step
  - Fabricate in-house
  - Rely on trusted Fabs
- Detect Trojan presence
  - Reverse Engineering
  - Exhaustive Testing
  - Side-Channel measurements

Side-Channel Techniques

Detection of Trojans through changes to secondary measurements such as:

- power consumption
- critical path timing
- light emission
- electromagnetic measurements

These techniques rely on a Trojan having a large impact.

- What are the limits of their effectiveness?
- How much can they detect?
- *What is the smallest Trojan they can detect?*

Process Variation

The largest obstacle to detection: Process Variation.

- Timing measurements are unreliable
- Leakage current varies by 5-10 times
- Total power varies by up to 50% [5]

What can we detect?

Where do we draw the line?

[5] S. Borkar, "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation," *IEEE Micro*, vol. 25, no. 6, pp. 10–16, 2005

Trojan Size

Some example Trojans have shown to be very small

- Even as low as 0.1% of total gate count in a LEON3 Processor [6]
- Around 0.1% to 0.4% increase in power/area in a MC-8051 microcontroller[7]

However, each Trojan affects each circuit differently.

- What is the cost (in area/power) to implement a Trojan?
- Is there a minimum cost?

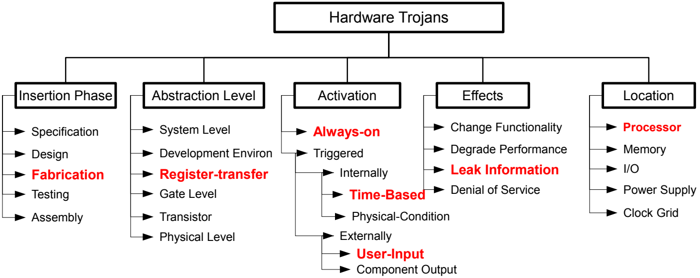
[6] S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, "Designing and implementing malicious hardware," in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET '08)*, 2008

[7] T. Reece, D. Limbrick, X. Wang, B. Kiddie, and W. Robinson, "Stealth assessment of hardware trojans in a microcontroller," in *IEEE 30th International Conference on Computer Design (ICCD '12)*, 2012-Oct. 3, pp. 139–142

Table (2). Trust-HUB Trojans on a 128-bit AES circuit

Trojan #	Trigger/Payload
AES-T100	*Always leak key covertly over many clock cycles*
AES-T200	*Always leak key covertly over many clock cycles*
AES-T300	*Leak parts of key intermittently*
AES-T400	*Always leaks key over RF*
AES-T500	*Drains the battery over time (not tested)*
AES-T600	*Always leak key covertly through leakage current*
AES-T700	*Leaks key after detecting specific sequence*
AES-T800	*Leaks key after detecting specific sequence*
AES-T900	*Leaks key after set number of clock cycles*
AES-T1000	*Leaks key after detecting specific sequence*
AES-T1100	*Leaks key after detecting specific sequence*
AES-T1200	*Leaks key after set number of clock cycles*
AES-T1300	*Leaks key after detecting specific sequence*
AES-T1400	*Leaks key after detecting specific sequence*
AES-T1500	*Leaks key after set number of clock cycles*
AES-T1600	*Always leaks key over RF*
AES-T1700	*Always leaks key over RF*
AES-T1800	*Drains the battery over time (not tested)*
AES-T1900	*Drains the battery over time (not tested)*
AES-T2000	*Leaks key after detecting specific sequence*
AES-T2100	*Leaks key after set number of encryptions*

Hardware Trojans



Understanding the Implementation Cost of Trojans

Trust-HUB Trojan 128-bit AES cryptographic circuit:

- 18 different implementations of data-leaks
- Identical host-circuit

What is the minimum Trojan impact?

Results: **There is no meaningful minimum impact**

Understanding the Implementation Cost of Trojans

Trust-HUB Trojan 128-bit AES cryptographic circuit:

- 18 different implementations of data-leaks
- Identical host-circuit

What is the minimum Trojan impact?

Results: **There is no meaningful minimum impact**

Methodology

1. Circuits were synthesized to standard cell libraries
2. Trojan circuits were compared to clean circuits to identify:
    - Changes in area
    - Differences in leakage power
    - Differences in dynamic power

Tools

These results were observed with

- Synopsys Design Compiler
- Cadence RTL Compiler

When synthesized to

- Synopsys 90-nm Cell Library
- OSU 45-nm Cell library

Impact on Area

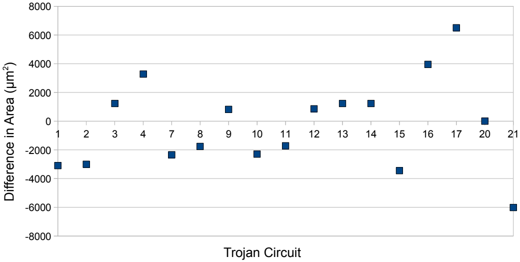


Figure (3). Footprint when synthesized to the Synopsys 90-nm cell library

Impact on Area

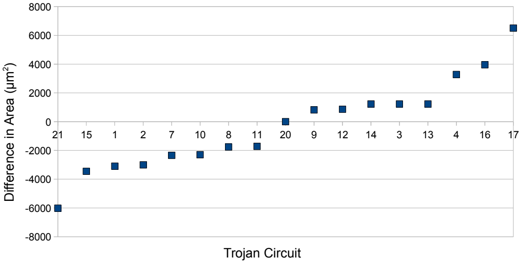


Figure (4). Footprint when synthesized to the Synopsys 90-nm cell library

The impact on area had a very even spread, with no observed "minimum".

Impact on Area

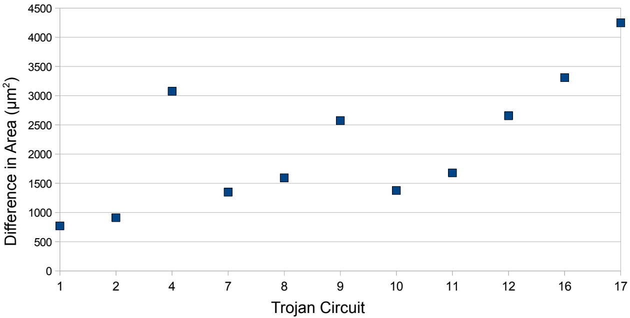


Figure (5). Footprint of Trojan circuits in area (μm^2) when synthesized to the OSU FreePDK 45-nm cell library.

Impact on Leakage Power

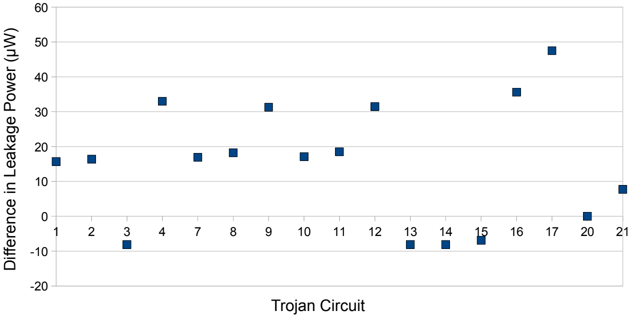


Figure (6). Footprint of Trojan circuits in leakage power (μW) when synthesized to the Synopsys 90-nm library.

Impact on Leakage Power

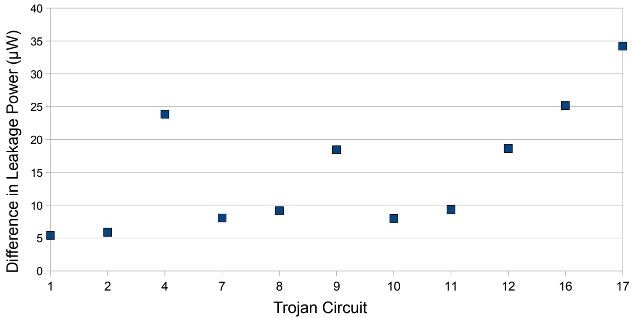


Figure (7). Footprint of Trojan circuits in leakage power (μW) when synthesized to the 45-nm OSU FreePDK cell library.

Impact on Dynamic Power

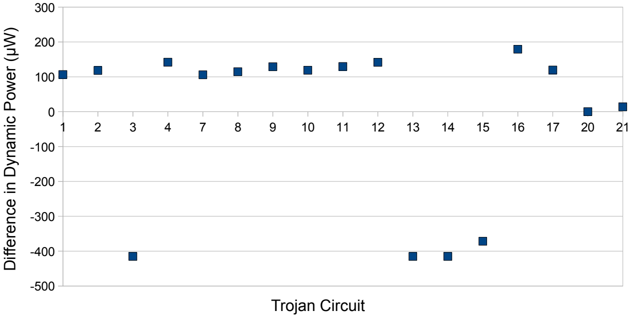


Figure (8). Footprint of Trojan circuits in dynamic power (μW) when synthesized to the Synopsys 90-nm library.

Impact on Dynamic Power

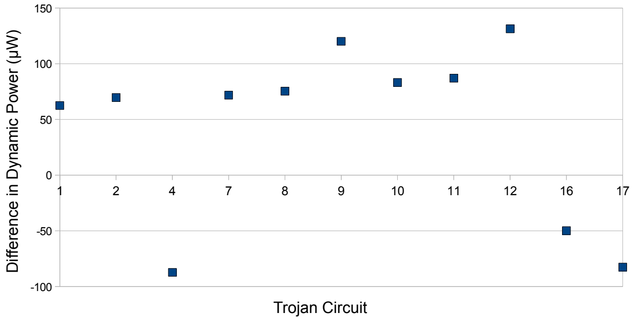


Figure (9). Footprint of Trojan circuits in dynamic power (μW) when synthesized to the 45-nm OSU FreePDK cell library.

Summary of results - 90-nm Library

Area

- Even spread between -6,018 μm^2 and 6,506 μm^2
- +/- 6,000 represents 0.4% of the clean area
- Absolute average impact was closer to 0.16%

Leakage Power

- Impact between 6.9 μW and 47.5 μW
- Percent impact varied between 0.19% and 1.34%

Dynamic Power

- Even spread between 13.9 μW and 415 μW
- Percent impact varied between 0.2% and 6%

Summary of results - 45-nm Library

Area

- Impact between 770.1 μm^2 and 4,247 μm^2
- Percent impact varied between 0.28% and 1.56%

Leakage Power

- Impact between 5.4 μW and 34.1 μW
- Percent impact varied between 0.17% and 1.05%

Dynamic Power

- Even spread between 49.8 μW and 131 μW
- Percent impact varied between 0.29% and 0.77%

Key Findings

There were several key results:

- Very small footprints
- No fixed cost
  - Widely varies even for similar Trojans
- Cost is dependent upon designer, not Trojan
- Differences in timing were so small that they could not be distinguished with the granularity of the software.

Questions?

- C. E. Irvine and K. Levitt, "Trusted hardware: Can it be trustworthy?" in *44th ACM/IEEE Design Automation Conference (DAC '07)*, 2007, pp. 1–4.
- D. Collins, "DARPA Trust in IC's Effort (BRIEFING CHARTS)," 2007.
- Semiconductor and Manufacturing Design Community, http://semimd.com/blog/2012/02/10/umc-seeks-to-shed-image-as-'fast-follower'/.
- R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans," *Computer*, vol. 43, no. 10, pp. 39–46, 2010.
- S. Borkar, "Designing reliable systems from unreliable components: the challenges of transistor variability and degradation," *IEEE Micro*, vol. 25, no. 6, pp. 10–16, 2005.

- S. T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou, "Designing and implementing malicious hardware," in *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET '08)*, 2008.
- T. Reece, D. Limbrick, X. Wang, B. Kiddie, and W. Robinson, "Stealth assessment of hardware trojans in a microcontroller," in *IEEE 30th International Conference on Computer Design (ICCD '12)*, 2012-Oct. 3, pp. 139–142.