Hardware integrity: from design to characterisation

Jacques Fournier – Bruno Robisson
Secure Architectures & Systems (SAS) laboratory
Fake/cloned/counterfeit products...

- Buying a fake branded handbag for your loved one?
- Finding horse meet in your beef lasagna?
- Fake portable hard drive?
- Having easy access to counterfeit medicines?
- Counterfeiting accounts for 2% of the world trade!
  Expected to exceed $1.7 trillion by 2015!
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC

- Context

- Existing solutions

- PUFs used for IC authentication

- Detection of corrupted hardware by physical means
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC
- Context
- Existing solutions
- PUFs used for IC authentication
- Detection of corrupted hardware by physical means
The corrupted, the counterfeit & the cloned IC

- This is your original chip... running your critical, sensitive operation...
The **corrupted**, the counterfeit & the cloned IC

- The corrupted chip is *your original chip* to which some malicious hardware has been added for, say,
  - Denial of service
  - Outputting sensitive data

We also refer to such malicious hardware as *Trojan Horses*
The corrupted, the **counterfeit** & the cloned IC

- The counterfeit is an exact copy of your original chip...
  - doing the same operations...
  - ... sometimes from the same manufacturer
The corrupted, the counterfeit & the cloned IC

- The ‘functional’ clone is another chip doing the same critical & sensitive operations as your original chip...
  - May be the same chip as your original one but with downgraded features.
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC

- Context

- Existing solutions

- PUFs used for IC authentication

- Detection of corrupted hardware by physical means
Context... some examples

Fake & genuine Atmel chips

Genuine & Fake Toshiba transistors

Fake chips sold to US military in 2010 (VisionTech scandal)
Context... another example

When a bank terminal or ATM machine is presented with a card, how can it know that...

- it is a genuine card?
- it is a functional clone?
- it is a compromised card?

Context... the supply chain

- A simplified version of the story...

*How far is everything under control? Who can you trust?*

Some ‘accelerating’ factors:
- Delocalisation of production sites to foreign countries
- Increasing number of ‘design houses’
- More & more value-added chips
- More and more complexe systems
- ‘Throw old & buy new’ of modern electronic devices
Context... some figures

- Counterfeit products (in general) represent 10% of the goods sold worldwide
  - Costs around $200b in the US each year...
  - ...which represents 250K job losses!

- It was estimated that the cost of counterfeiting and piracy for G20 nations was between $450 and $650 billion in 2008 and will grow to $1.2 to 1.7 trillion in 2015

- For the semiconductor industry, the counterfeit market is estimated at 7% of the whole market, representing approx. $10b of loss for the industry each year.
Context... a few stories

- In 2006 **fake NEC company** unveiled in China.
  - Over 50 counterfeit products were produced there!

- In 2007, **hacked payment terminals** found in the UK.
  - Extra hardware had been inserted to store card data and PIN and send them to Pakistanis servers

- Between 2006 & 2010, **VisionTech Components** knowingly sold counterfeit ICs to approx. 1,101 customers WW.
  - including counterfeit ICs for military applications.

- In 2011, the Chinese company **Huawei** was excluded from the public safety broadband network projects.
  - Risk of hidden functions to disrupt or intercept (American) communications.

- In 2011, a virus infected the cockpits of America’s **Predator and Reaper drones**.
  - logging pilots’ every keystroke during fly missions over Afghanistan and other warzones.

- A few on going initiatives:
  - The **Trusted Foundry Program**: [www.trustedfoundryprogram.org](http://www.trustedfoundryprogram.org)
  - The **Trust in IC** program: started by the DARPA in 2007 to develop efficient methods for Hardware Trojan detection.
  - The **ENISA** (European Networks and Information Security Agency) initiated in 2011 an action towards securing the Supply Chains of electronics security devices.
Context... the consequences

- Market loss... with the potential impact on the job market!
- Damaging brand image & customer satisfaction
- Downgraded security
- Downgraded reliability
- Potential impact on the environment
  - ‘Out-of-regulation’ production, disposal etc
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC

- Context

- Existing solutions

- PUFs used for IC authentication

- Detection of corrupted hardware by physical means
Existing solutions

- Visual inspection!

- PUF-based authentication
  - Retrieving a digital « fingerprint » of a circuit (*we’ll come back to that later*)

- Obfuscation
  - ‘Obfuscation’ of the HDL code
  - Hardware ‘random’ Place & Route.

- Watermarking
  - Similar to watermarking of a software, a picture, a movie...
  - Objective is to add a « hidden » characteristic within the circuit
Existing solutions (cont’d)

- ‘Cryptographic’ activation of the chip...
- ... or restricting access to some parts of the chip
- Obfuscation of finite state machines
- Dynamique encryption of bit streams (for FPGAs)
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC
- Context
- Existing solutions
- PUFs used for IC authentication
- Detection of corrupted hardware by physical means
PUFs used for IC authentication

- Say we have 2 ‘identical’ circuits from the same manufacturer...

- Those two circuits have subtle differences due to technological & fabrication processes
PUFs used for IC authentication

- A ‘Physically Unclonable Function’ (PUF) is a function which should allow to measure a characteristic « biometric data » of the circuit...

Those two have (different colours 😊) but also different « fingerprints »

Main Properties
- Unique
- Non predictable
- Stable wrt environmental conditions
- ...tamper evident

Some examples
- Non predictable SRAM state upon power on
- Subtle differences in the frequency of two ring oscillators
- Arbiter based race conditions of two paths
- ...
PUFs used for IC authentication

TWO APPROACHES

Design issues with (Silicon) PUF implementations
- Most existing research work rely on simulations or FPGA implementations.
- Very few existing ASIC implementations (UNIQUE project).
- But extremely difficult to do in industry (full custom design, careful layout etc).

Resistance of proposed PUFs to physical attacks
- Proposed PUFs satisfy the properties of uniqueness, stability & non reproducibility in theory.
- Use physical attacks (power, EM, temperature, Vcc glitches) to corrupt those PUFs

Use Vcc variations to make one PUF behave just like another one
Use power analysis to infer the value of the supposedly secret outputs of the PUF
Use temperature variations to bias the output of the PUF

We are working on the design of Arbiter PUFs and studying the compromise between the level at which design has to be done ‘by hand’ and reaching the security properties of PUFs.
Hardware integrity: ...

- The corrupted, the counterfeit & the cloned IC

- Context

- Existing solutions

- PUFs used for IC authentication

- Detection of corrupted hardware by physical means
Detection of corrupted hw by physical means

- Our approach is to use side channel measurements to detect the hardware Trojan or detect its effect... before it is too late

Objective is to use power consumed by the chip or the Electromagnetic emissions of the chip to detect the presence of the Trojan

Already an extensive literature on the subject, but most approaches detect the 'effect' of the Trojan, i.e. once your critical data has been leaked!!

We are developing a method based on Fault injections to detect modifications incurred by the presence of the Trojan on the circuit even if it is not active
Detection of corrupted hw by physical means

- Our approach is to use side channel measurements to detect the hardware Trojan or detect its effect... before it is too late

Fault injections are usually used to corrupt sensitive operations to, say, retrieve cryptographic keys!

But we showed that fault injections can also be used to ‘characterize’ a circuit, for e.g. measure sensitive data delay paths (w. clock glitches)

“The good & the bad of physical functions”

We measure ‘faults generated’ for several values of clock glitches’ values & define caracteristic s.

Difference between the distribution variation on genuine circuit & that of the same circuit with a hardware Trojan
To conclude...

- (Inter)national security issues
- Safety issues
- Billions of euros at stake for the semiconductor industry
- Impact on the environment

It matters for...

- Rocket
- Credit card
- Airplane
- Car
- Medical device
Merci de votre attention