Salutary Hardware to Design Trusted IC
Lilian Bossuet
Université de Lyon – Laboratoire Hubert Curien – UMR CNRS 5516 – Saint-Etienne, France

Ecole d’hiver Francophone sur les Technologies de Conception des Systèmes embarqués Hétérogènes
January 2014, Ottawa, Canada
SALWARE

why ?
Main threats

- Intellectual properties theft
- Mask, chip and device theft
- Overbuilding
- Illegal copy, cloning
- Counterfeiting
- Illegal refurbishing, repackaging, relabeling
- Reverse engineering
- Functional modifications (DRM violation, unlocking)
Definition

A) Original chip, package and label

B) Same chip, other package and other label (chip theft, repackaging)

C) Same chip and package, other label (IC theft, relabeling)

D) Used chip, refurbished package and label (Chip salvaging)

E) Other chip, same package and label (IC counterfeiting)
Example of counterfeiting flash memory

One counterfeit device (left) had Toshiba markings but a Samsung die inside. You can see the actual Toshiba device markings on the second device. The Samsung die can be seen in the third image.

Source: EE Times, August 2007
The rise of electronic device counterfeiting

Target and evolution
– From US statistical studies [1-2]


Fake NEC company found, says report
SALWARE

what ?
Salutary hardware to design trusted IC

**SALWARE definition**

Salutary hardware (SALWARE) is a (small piece of) hardware system, hardly detectable (from the attacker point of view), hardly circumvented (from the attacker point of view), inserted in an integrated circuit or an IP, used to provide intellectual property information and/or to remotely activate the integrated circuit or IP after manufacture and/or during use.
Malware definition

Malicious hardware *(MALWARE)* is a *(small piece of)* hardware system, hardly detectable *(from the user point of view)*, hardly circumvented *(from the user point of view)*, inserted in an integrated circuit or an IP, used to provide *attacker hidden information* and/or to remotely inactivate the integrated circuit or IP after manufacture and/or during use.

Hardware Trojan

- Small, hardly detectable
- Disable a part of a device => remote activation
- Information leakage => IP watermarking
- Time-based activation mechanism => IP expire date (temporary license)

Backdoors

- Malicious / salutary ???

Side channel

- Typical SCA attacks on cipher => IP watermarking
- Trojan detection
Side-channel attacks

- Side-channel key recovery (side-channel)
  - Attacker aims to get back the secret key
Example

- Side channel used to IP protection
  - IP information transmission
    - ID (from PUF)
    - Watermark

- Side channel to send IP watermarking
  - EM Channel (contactless, local)
  - BFSK transmitter (logical)
    - 200 / 300 Mhz
  - Adapted to FPGA implementations
    - Tests in progress
    - Microsemi / Altera

![Diagram showing IP identification (PUF, watermarking) and Hardware Trojan activation.](fetch2014)
Example

Circuit A - 8 bits counter and binary code
Circuit B - 8 bits counter and Gray code
Circuit C - 8 bits counter and binary code with Sbox
Circuit D - 8 bits counter and Gray code with Sbox
Circuit E - 8 bits counter and binary code with Sbox and Wk
Circuit F - 8 bits counter and Gray code with Sbox and Wk

Side channel used to IC protection
- Counterfeiting detection
  - Watermarking checking
    - Illegal IP/IC copy
    - Fingerprinting
- Power consumption (cheap, global)
- Adaptation of the CPA (Correlated Power Analysis) attack
- Experimentations
  - 6 counters (worst case)
  - FPGA implementations
  - FSM finder

Example
Salware / Malware

**Salutary Hardware vs Malicious Hardware**

- Hidden remote access
- Information leak (side channel)
- PUF watermark (side channel)
- Secure remote access

Investigating **MALWARE design and behavior as a opportunity to improve SALWARE**
http://www.univ-st-etienne.fr/salware/
Blocage fonctionnel

Actions de blocage dans un SoC

– Contrôleur (FSM / interruption / mémoire)
– Réseaux de communications internes : bus de données / Cross Bar / NoC
– Mémoires RAM (bus @ / bus data)
– Paramétrage/calibration (bloc analogique et mixte)
– Configuration (eFPGA / multi-mode-IP)

Source STMicroelectronics – STW22000 microcontroller
Counterfeiting in figures

- 10% of the global word market
  - Cost: 200 billion $ per year in USA
  - Impact: 250,000 employments loss per year in USA

In 2008, the number of counterfeiting seizures of the European customs was 178 million of products.
  - Watch, leather goods, article of luxury clothing, medicine, tabacco, electronics products

Estimation of counterfeiting of the word semiconductor market is around 7% [1]
  - Financial loss of 10 billion $ per year for the word market

From 2007 to 2010, the number of seizures of electronic devices counterfeiting of the US customs was 5.6 million [2]
  - Numerous counterfeiting of military-grade device and aerospace device [3,4]

---

   www.trustedfoundryprogram.org
Trojan insertion for IP protection during evaluation

- Case Western Reserve University
- Trojan insertion by IP’s FSM modification
- Re-synthesis of IP with Trojan
- Time-activated Trojan
- Trojan signature use as a digital watermarking (in case of illegal IP copy)