SALWARE

Salutary Hardware to Design Trusted IC

Lilian Bossuet¹, David Hely²

¹ – Université de Lyon – Laboratoire Hubert Curien – UMR CNRS 5516 – Saint-Etienne, France
² – Grenoble Institut of Technology – Laboratoire LCIS – EA CNRS 3747 – Valence, France

TRUDEVICE Workshop 2013
May 30-31, Avignon France
Trustworthy manufacturing

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)
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.or
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**

1. **Setting the International Standard(s) in the FIGHT AGAINST COUNTERFEITS**
2. **Supply-Demand-Chain Executive**
3. **Counterfeit Crisis**
4. **EE Times**

**Target**

- Transistors (25% consumers)
- Programmable Logic (30% industry)
- Memory (53% computer)
- Micro-processors (85% computer)
- Analog devices (29% wireless)
- Others

**Counterfeits**

- **Fake NEC company found, says report**
- **Supply Chain Best Practices**
- **Fighting the Fakes**

**Evolution**

- From US statistical studies [1-2]

---

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.
Salutary hardware to design trusted IC

**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
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)

Salware / Malware

Salutary Hardware vs Malicious Hardware

Investigating MALWARE design and behavior as a opportunity to improve SALWARE
TRUDEVICE Workshop 2013
May 30-31, Avignon France
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)