SALWARE

Salutary Hardware to Design Trusted IC

Lilian Bossuet[1], David Hely[2]

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

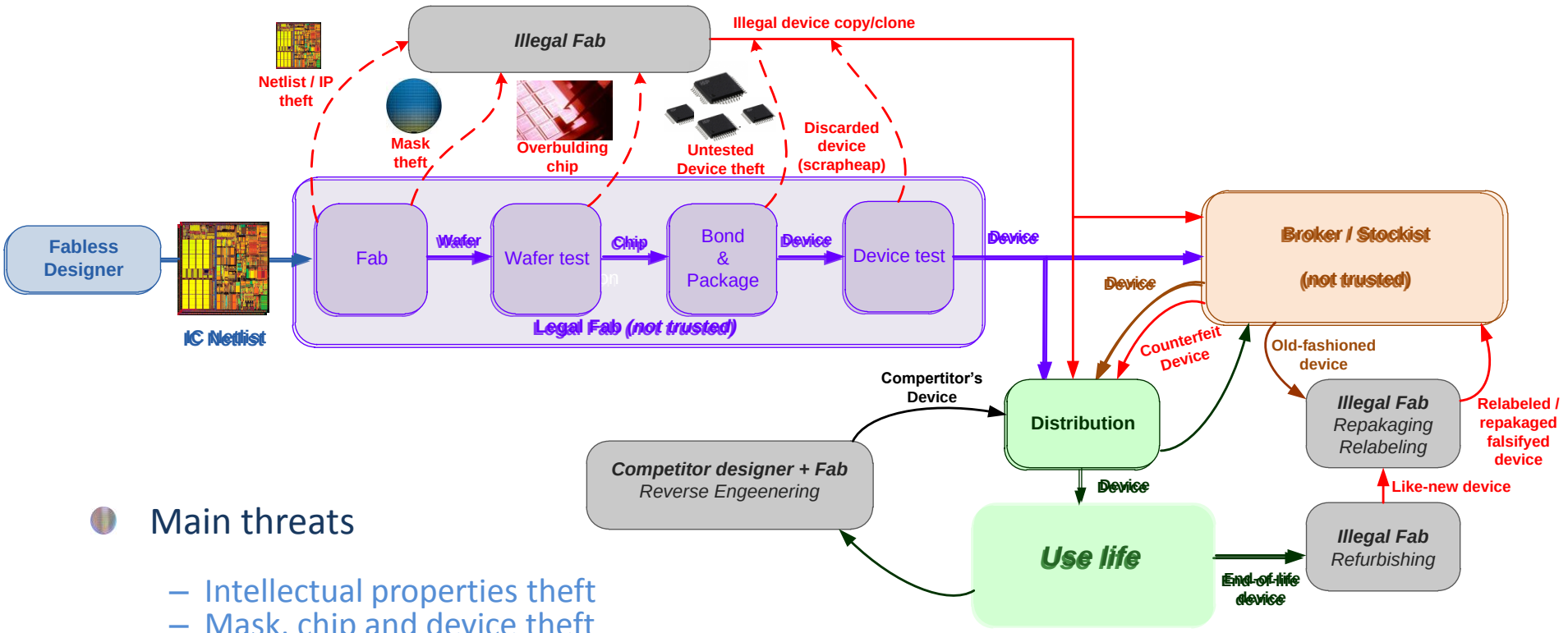
TRUDEVICE Workshop 2013

May 30-31, Avignon France

Trustworthy manufacturing

why ?

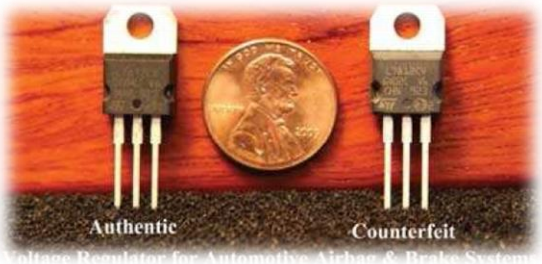
Threat model during manufacturing, supply chain and use life



- 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)

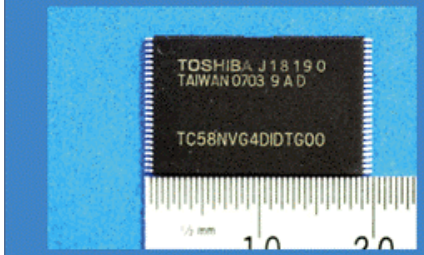
Counterfeiting in figures

- 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]



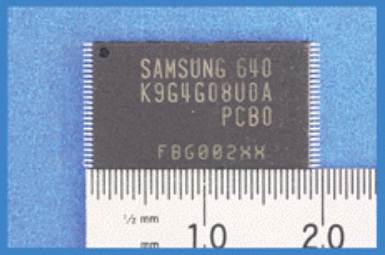
[1] M. Pecht, S. Tiku. Bogus! Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, May 2006
[2] AGMA, Alliance for Gray Markets and Counterfeit Adatement, http://www.agmaglobal.org
[3] S. Maynard. Trusted Foundry – Be Safe. Be Sure. Be Trusted Trusted Manufacturing of Integrated Circuits for the Department of Defenses. NDIA Manufacturing Division Meeting, October 2010
www.trustedfoundryprogram.or
[4] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012

Example of counterfeiting flash memory

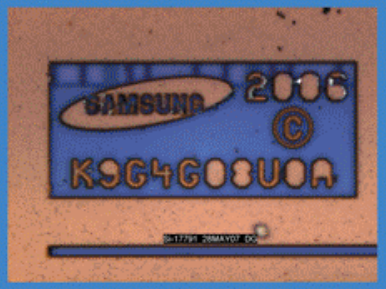


Counterfeit Toshiba Part Package Marking TC58NVG4D1DTG00

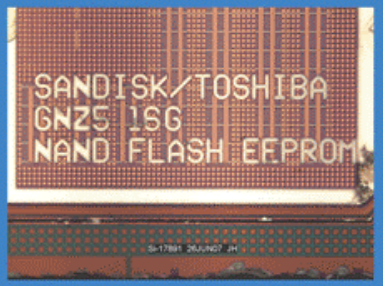
Toshiba 56nm 16Gb MLC NAND Flash Part Package Marking TC58NVG4D1DTG00



Samsung 65nm 4Gb MLC NAND Flash Part Package Marking K9G4G08U0A



Counterfeit Toshiba Part Die Markings



Toshiba 56nm 16Gb MLC NAND Flash Part Die Markings

Samsung 65nm 4Gb MLC NAND Flash Die Markings

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 counteirfetings

- Target and evol

dies [1-2

Analog devices (29% wireless)

Micro

uter)

ry)

Nombre de références saisies

12

600

300

0

2001 2002 2003 2004 10

[1] C. Gorman. Counterfeit Chips on the Rise. IEEE Spectrum, June 2012
[2] IHS-ERAI http://www.ihs.com/info/sc/a/combating-counterfeits/index.aspx

LABORATOIRE Hubert CURIEN
UMR • CNRS • 5516 • ST-ETIENNE

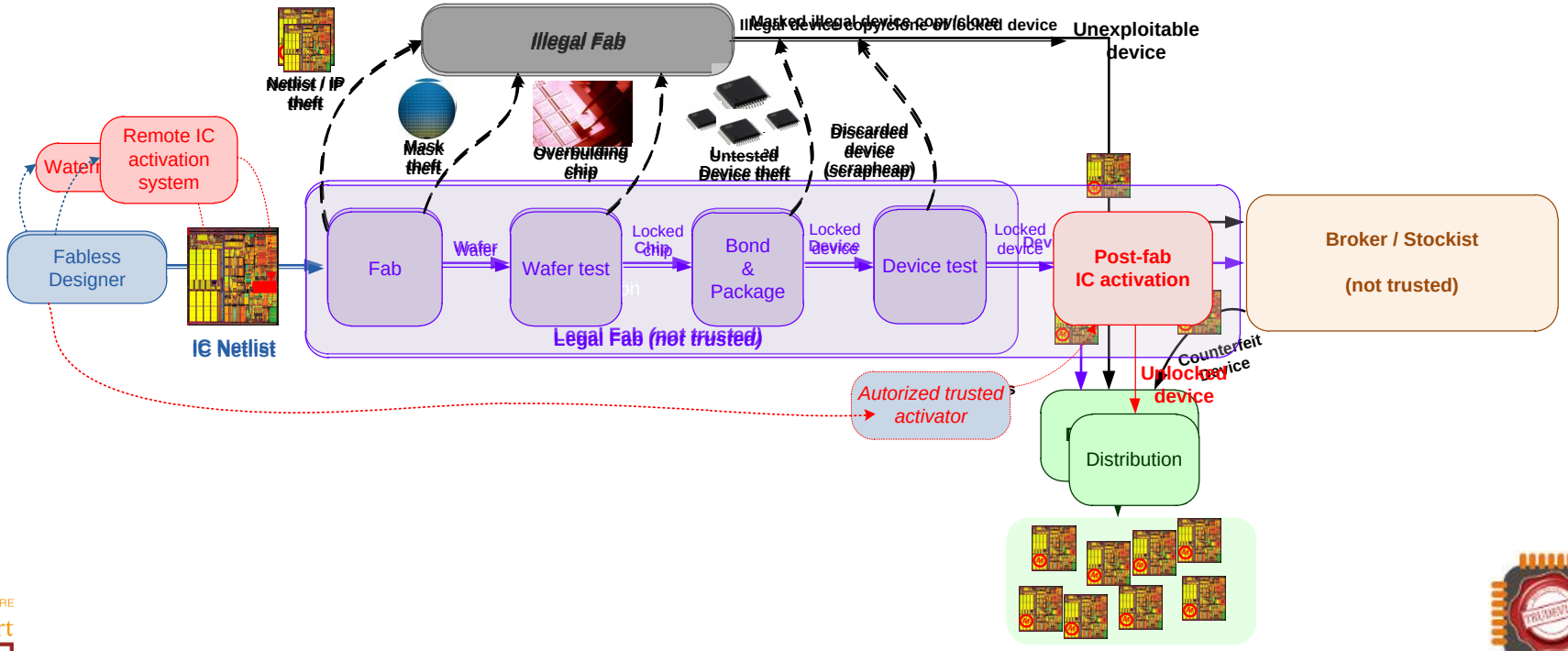
SALWARE

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.

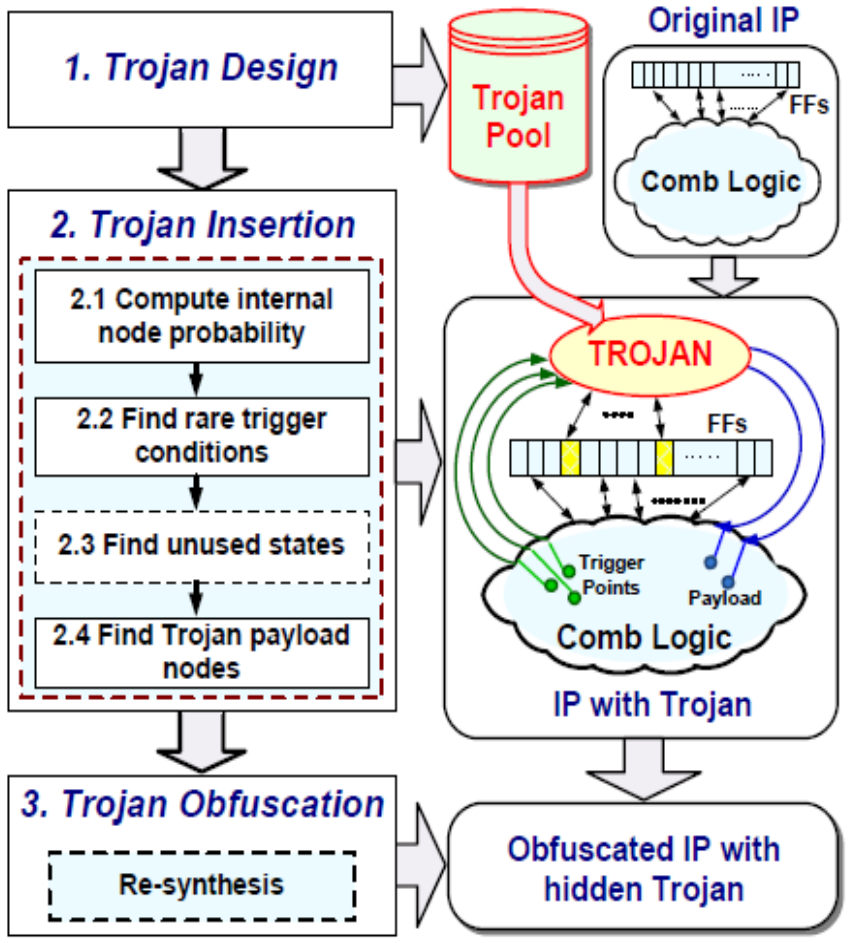
- Hardware Trojan
  - Small, hardly detectable
  - Disable a part of a device => remote activation
  - Information leakage => IP watermarking
  - Time-based activation mechanism => IP expire date (temporary license)

- Backdoors
  - Malicious / salutary ???

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

Exemple

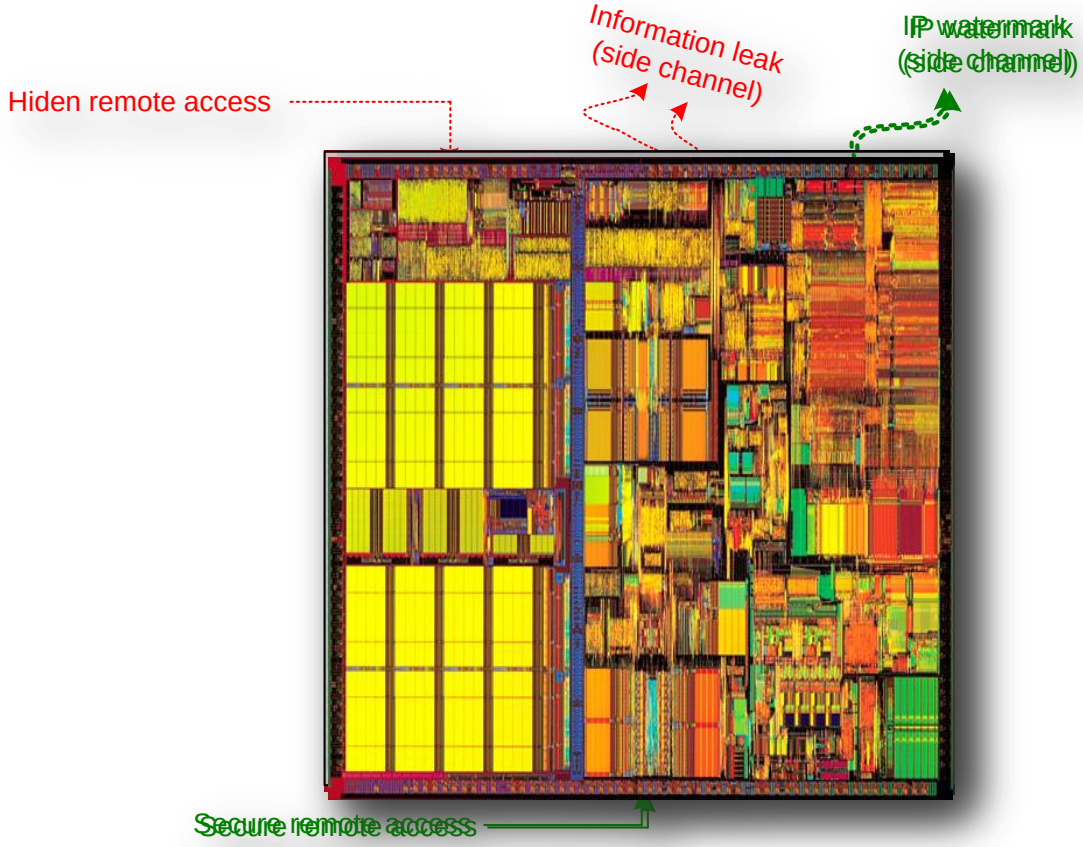
- Trojan insertion for IP protection during evaluation
  - Case Western Reserve University
  - Trojan insertion by IP's FSM modification
  - Re-synthesis of IP with Trojan
  - Time-activated Trojan
  - Trojan signature use as a digital watermarking (in case of illegal IP copy)



[1] Seetharam Narasimhan, Rajat Chakraborty, Swarup Bhunia, "Hardware IP Protection During Evaluation Using Embedded Sequential Trojan," IEEE Design & Test of Computers, 08 June 2011.

Salware / Malware

- *Salutary Hardware* vs *Malicious Hardware*



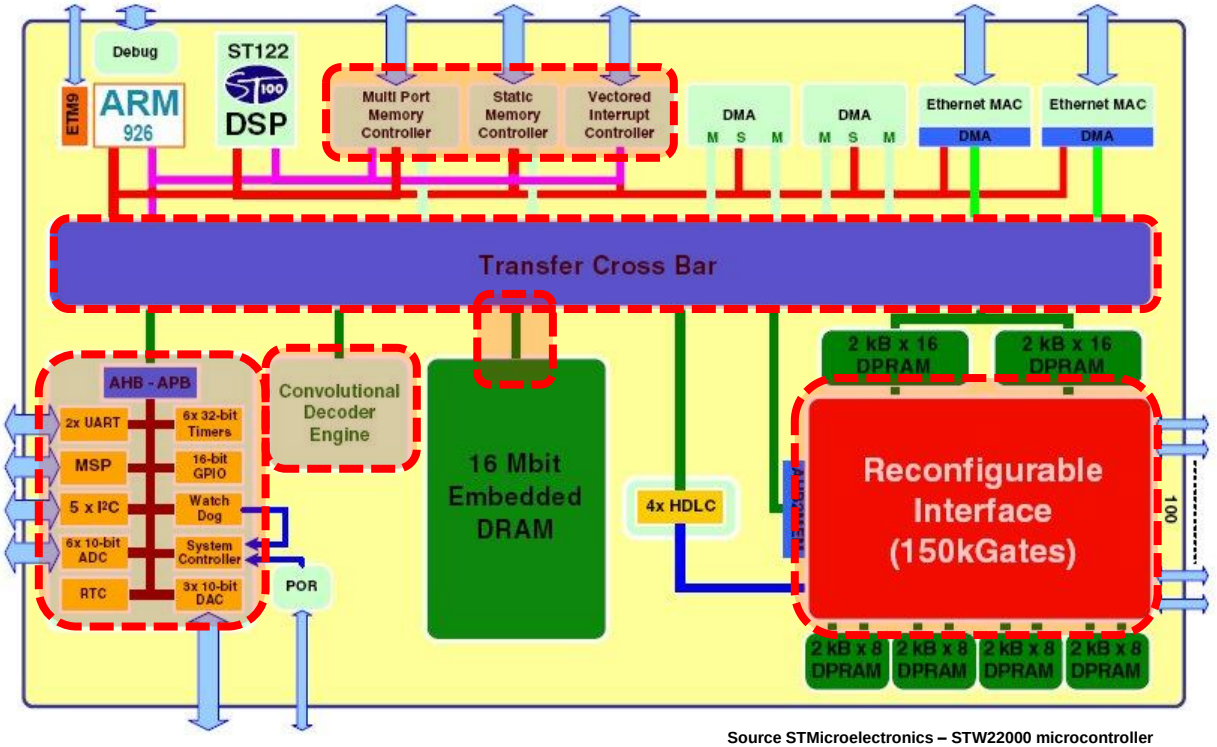
- *Investigating MALWARE design and behavior as a opportunity to improve SALWARE*

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)



Source STMicroelectronics – STW22000 microcontroller