Technology

Security Challenges and Requirements for Industrial Control Systems in the Semiconductor Manufacturing Sector

Malek Ben Salem

Accenture Technology Labs

NIST Workshop on Cyber-Security for Cyber-physical Devices

April 23rd, 2012

High performance. Delivered.

accenture

consulting | technology | outsourcing

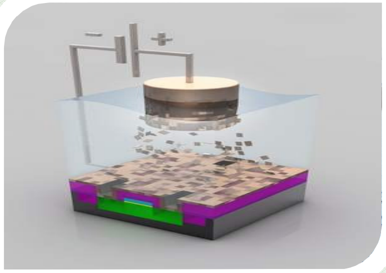
Outline

- Background Information
- Security Challenges
- Sample Attack
  - Insertion of Hardware Trojans
  - Failure of Existing Common Hardware Trojan Detection Approaches
- Research Priorities
- Summary

Semiconductor Manufacturing: Background Information

Chip Manufacturing Process Overview

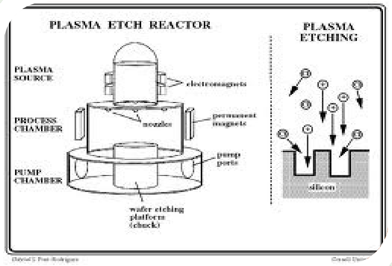
Semiconductor device fabrication is a series of four types of processing steps: deposition, etching, patterning, and modification of electrical properties. Additional measurement/metrology steps are added.



Deposition

Growing /transferring material onto wafer, wafer coating .

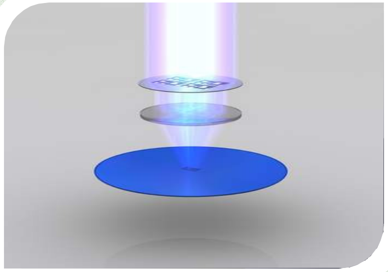
E.g. Wafers are put into a copper sulphate solution, and Copper ions are deposited onto the transistor through a process called electroplating.



Etching

Removing material from the wafer either in bulk or selectively process used between levels.

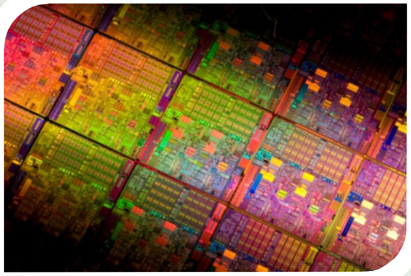
E.g. Chemical Mechanical Planarization (CMP)



Lithography

Patterning and shaping of wafer materials

E.g. wafer costing with a photo-resist that gets exposed by a stepper, a machine that focuses, aligns, and moves the mask exposing select portions of the wafer to short wavelength light.



Electrical Property Modification

Doping transistor sources and drains by diffusion furnaces and by ion implantation

Activating implanted dopants through Furnace or Rapid Thermal Anneal (RTA)

Pictures courtesy of spectrum.ieee.org, intel.com, and poli.cs.vsb.cz.

Trends in Semiconductor Manufacturing

- Moore’s Law and the market requirements for higher performance chips are driving the production of smaller transistors
  - Smaller devices and larger wafers
- Adoption of the e-Manufacturing paradigm
  - Fully-automated factories
- Control systems are more complicated
- Tighter tolerance windows
- More stringent process controls are implemented on semiconductor manufacturing processes and equipment

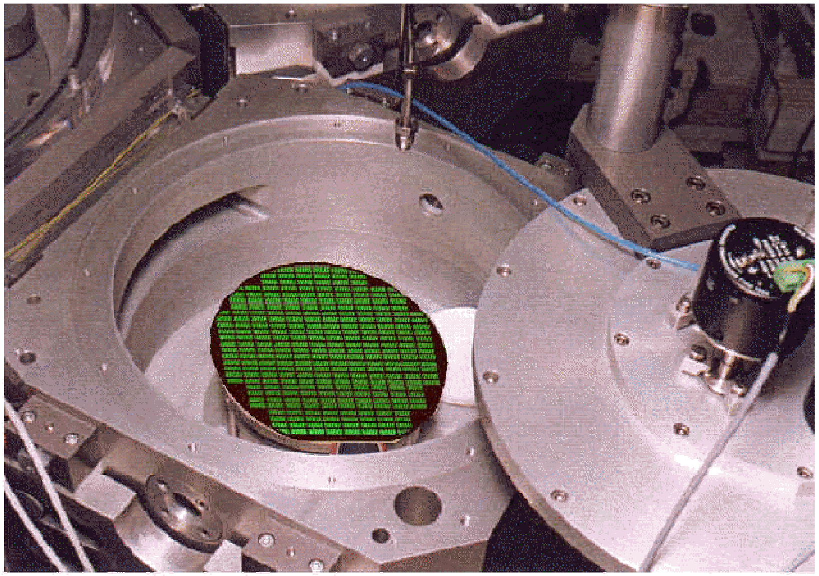
Trends in Semiconductor Manufacturing (contd.)

- Economic and market forces drive outsourcing IC fabrication
  - Compromising the IC supply chain for sensitive commercial and defense applications becomes easy.
  - Attacker could substitute Trojan ICs for genuine ICs during transit.
  - Attacker could subvert the fabrication process itself by implanting additional Trojan circuitry into the IC mask.
- Manufacturing Grid: Joint production platforms
  - Cyclic demand for consumer electronic products
  - High costs of development and production facilities for different technology node and wafer sizes
  - Load distribution among manufacturing partner facilities
- Objectives:
  - Optimize all the distributed manufacturing resources
  - Minimize IP disclosure

Security-Related Challenges

Equipment Control and Recipe Integrity

- Recipes:
  - Specifications of equipment processing
  - Used to control manufacturing equipment, including processing tool chamber temperature, pressure, and cooling/heating rates.



- Critical Security Issues
  - Trusted recipe content to ensure that the recipe on the equipment is exactly the one that the factory approved and selected.
  - Traceability of recipe items and parameter usage
  - Preventing DoS attacks and blocking the communication channels between equipment controllers and sensors or recipe databases

Picture courtesy of seconsemi.com

Process Data Integrity

- Advanced Process Controls (APC) are critical for high-quality process performance and factory yield
  - Feed-forward and feedback control
  - Automated fault detection to equipment and to the automated factory, in order to improve process performance and factory yield.
- These techniques, known as APC rely on the integrity of the data measured by equipment sensors.
  - Accurate sensor readings
  - Accurate and timely alarm reporting
  - Alarm reporting is critical to the safety of the equipment, the product, and the factory in general.

False Data Injection Attacks

- Malicious third party compromises the integrity of the control systems by controlling the readings of one or more sensors
  - e.g. sensors measuring the ambient temperature inside a chamber on an Ion implantation tool

- APC is vulnerable to false data injection attacks.
  - Consequence: scrapped wafers
- High scrap costs
  - Average wafer cost ~$9000 (depending on product and process step)
  - Wafers are processed in lots of 25 wafers
  - MWTD (Mean-Wafers-To-Detect) depends on sampling plan and process performance.

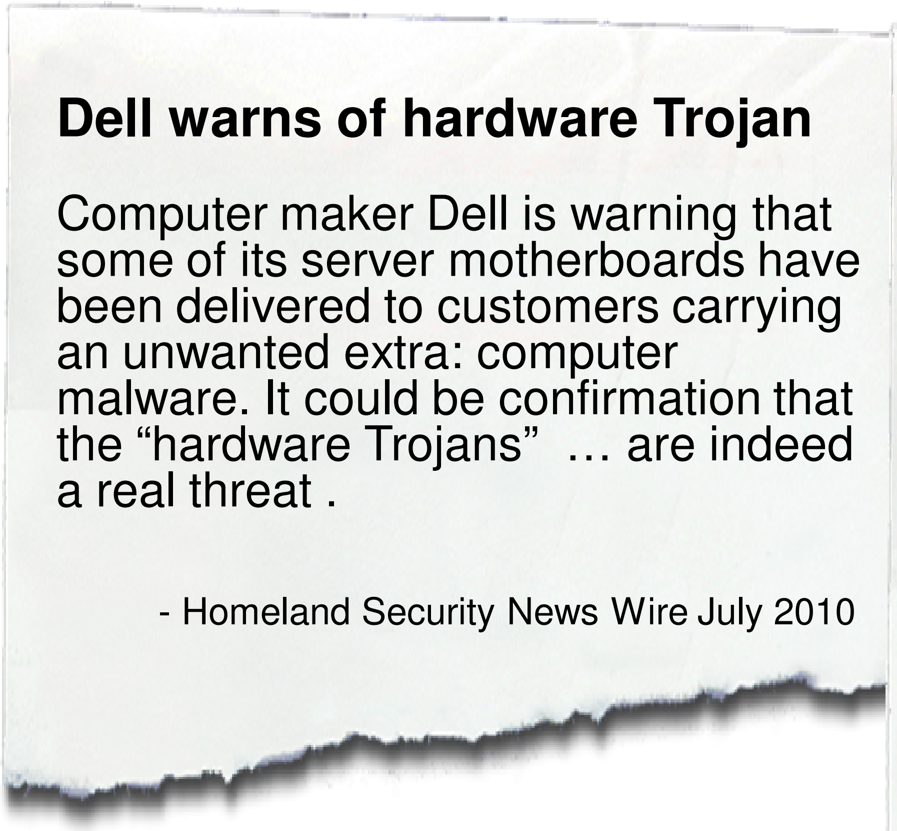
Picture courtesy of rubbertechnology.info

Privilege Over-Entitlement

- High job rotation rates
  - Process engineers rotate through various product wafer processing steps
  - Engineers rotate between design, process and integration roles
  - Complicated access controls management to product and equipment recipes
- Many engineers quickly accumulate privileges that they do not need to perform their current job functions.
- Highly-privileged access to equipment sensors and controllers is a serious threat
  - Serious problem, although not strictly related to cyber-physical devices
  - Exacerbated by remotely accessible control system, distributed global teams, and open specifications used for process equipment design.

Sample Attack:
Hardware Trojans

Hardware Trojans in the News



Dell warns of hardware Trojan

Computer maker Dell is warning that some of its server motherboards have been delivered to customers carrying an unwanted extra: computer malware. It could be confirmation that the “hardware Trojans” … are indeed a real threat .

- Homeland Security News Wire July 2010

F.B.I. Says the Military Had Bogus Computer Gear

…the .. sinister specter of an electronic Trojan horse, lurking in the circuitry of a computer or a network router and allowing attackers clandestine access or control, was raised .. by the FBI and the Pentagon.
The new law enforcement and national security concerns were prompted by Operation CISCO Raider, which has led to 15 criminal cases involving counterfeit products bought in part by military agencies, military contractors and electric power companies in the United States.

-The New York Times, May 2008

Hardware Trojans

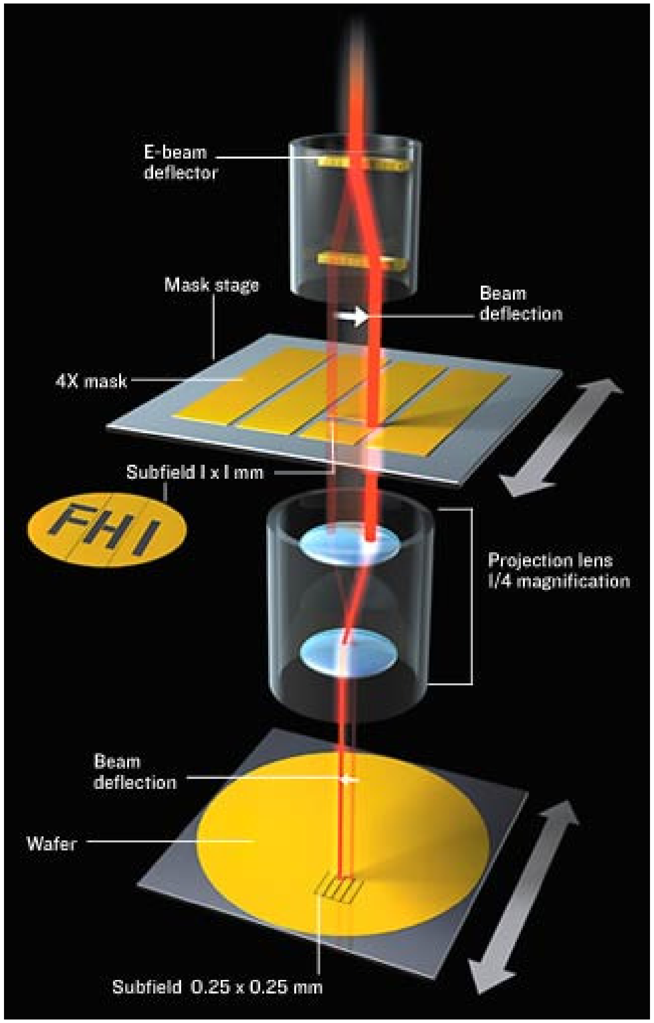
- Monitor for a specific but rare trigger condition
  - e.g., a specific bit pattern in received data packet or on a bus
  - until a timer reaches a particular value.
- Hardware is the root of trust
  - Software security mechanisms can be bypassed by malicious hardware.
- Potential targets
  - Hardware used for defense
  - Commercial grade cryptographic and security critical hardware
- Look genuine ICs with normal input/output behavior during testing and normal use.
- Tampering is very difficult to detect and mitigate
  - Hard to detect using visual inspection or conventional testing techniques

Hardware Trojans

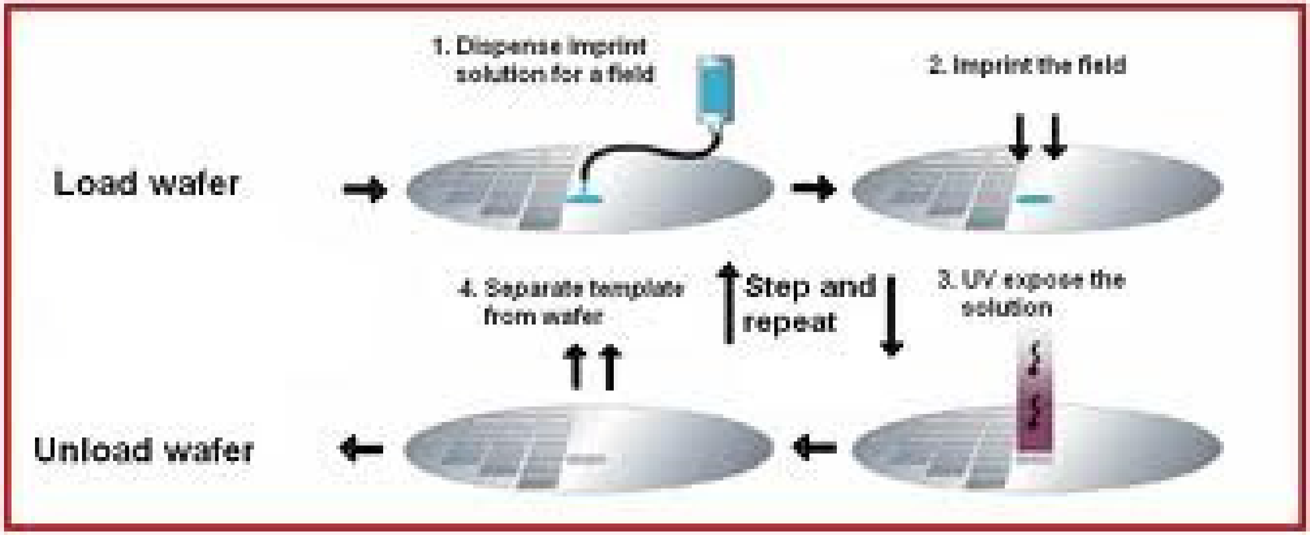
- Trojans may be inserted during the design or manufacturing
  - Long supply chain
  - Complexity increases vulnerability
- Capable of inflicting catastrophic damage
  - Modify chip’s function through additional logic or by removing or bypassing existing logic
    - Disabling encryption
    - Clock disruption to shut down the chip or affect its synchronization
    - Adding glitches to compromise system integrity and security (backdoor)
    - Destruction of the operating environment of original circuit
      - Shutting down power (kill-switch), generating noise to disrupt critical signals, or increasing thermal gradients on the chip possibly causing burn out
  - Modify chip’s parametric properties
    - E.g. delay by modifying wire and transistor geometries

Photolithography

- Process used to remove parts of a thin-film or substrate
- Uses light to transfer a geometric pattern from a photomask
- Includes several steps
  - Wafer Cleaning, Barrier Formation and Photoresist Application
  - Soft-Baking
  - Mask Exposure
  - Printing
  - Development
  - Hard-Baking

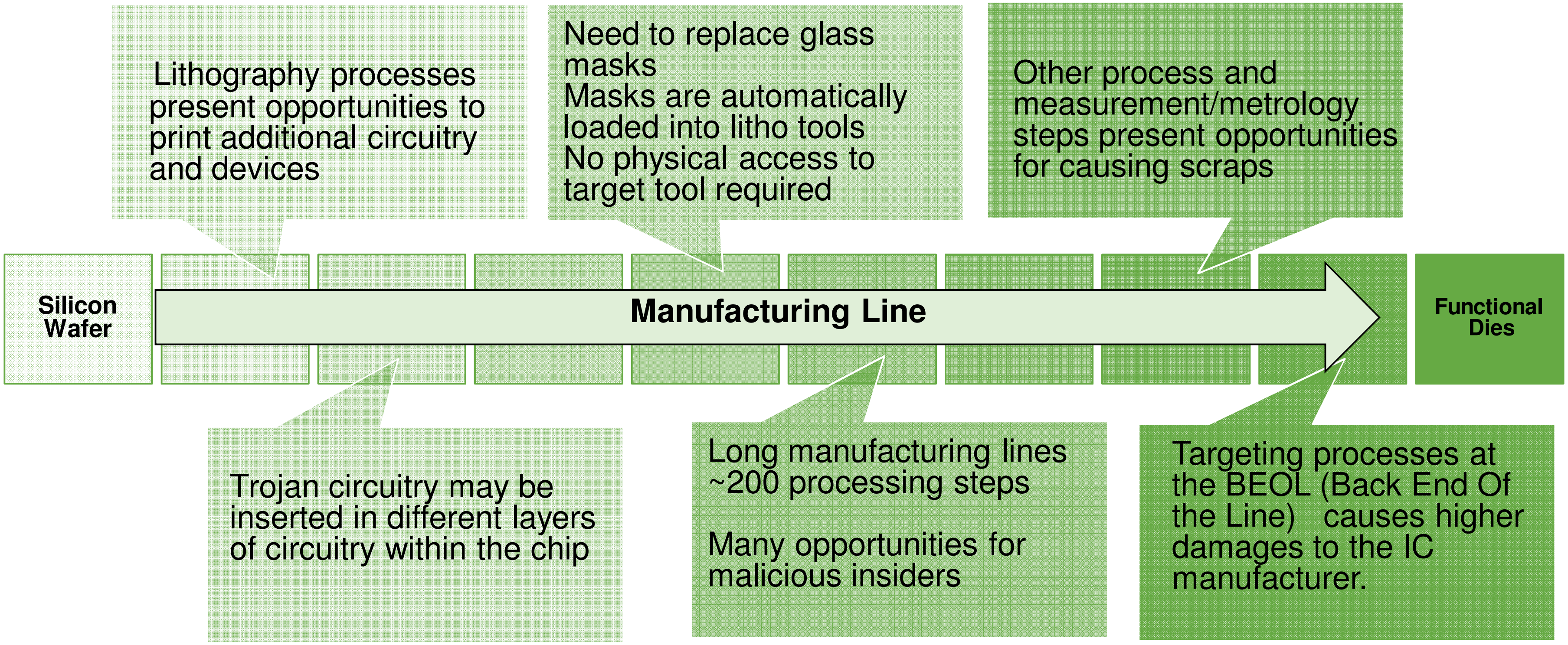


Conventional Multi-layer Lithography : Stepping


1. Dispense imprint solution for a field
2. Imprint the field
Load wafer
4. Separate template from wafer
Step and repeat
3. UV expose the solution
Unload wafer

- Composed of one patterning step and several steps of oriented deposition
- Most lithographic techniques are 2-dimensional (photolithography, e-beam lithography, and imprint lithography)
- Using the wrong mask affects all dies on a wafer
- All chemicals are loaded automatically into the tool, and controlled by recipe items.

Many Opportunities for Malicious Insiders



Lithography processes present opportunities to print additional circuitry and devices

Need to replace glass masks
Masks are automatically loaded into litho tools
No physical access to target tool required

Other process and measurement/metrology steps present opportunities for causing scraps

Trojan circuitry may be inserted in different layers of circuitry within the chip

Long manufacturing lines ~200 processing steps

Many opportunities for malicious insiders

Targeting processes at the BEOL (Back End Of the Line) causes higher damages to the IC manufacturer.

Transistors Formed from a Single Lithography Step [3]

- Topographically Encoded Micro-Lithography (TEMIL)
  - Single level of topography (photolithography or molding)
  - A substrate with multiple shadow evaporations
- Shadow Evaporation
  - All information needed to fabricate complex structures is encoded in the topography of patterned polymer
- May replace several steps of lithography
  - One lithography step
  - Sequential shadow evaporation/deposition steps of various materials
  - Each functional layer of device can be deposited independently using a single level of topography
- Produce transistors without any doping, etching, or lithography alignment steps
- Malicious insider needs access to one tool/recipe only

Hardware Trojan Activation

- Trigger Type
  - Ticking time-bomb triggers: Open to everyone
  - Data triggers: Hacker needs access to the machine to trigger
- Externally-activated
  - Using a receiver or antenna on chip
  - Forcing internal registers to specific date to extract secret keys
- Internally-activated
  - Always-on: Trojan continuously active, implemented by modifying the geometries of the chips, such that certain nodes or paths in the chip have a higher susceptibility to failure (parametric Trojans)
  - Condition-based (Temperature, pressure, or voltage sensor output / Internal logic state / Input pattern / Internal counter value.
    - Implemented by adding logic gates and/or flip-flops to the chip)
    - Represented as a combinational or sequential circuit

Failure of Existing Common Solutions

- Currently impossible to certify the trustworthiness of processors & controllers as Trojan detection is very hard
- Nano-scale devices and high system complexity make detection through physical inspection almost impossible.
- Inspection through destructive reverse engineering does not guarantee absence of Trojans in ICs not destructively inspected.
- Audits not very effective at catching bugs
- Obfuscation during fabrication
  - Motivated attacker can always identify criticality of manufactured IC
  - Shown to be impossible to achieve in most cases
- Triggers are finite state machines that can change states when **time** or **input data** changes

Trojan Detection: Failure Analysis

- Techniques
  - Scanning optical microscopy (SOM)
  - Scanning electron microscopy (SEM)
  - Pico-second imaging circuit analysis (PICA)
  - Voltage contrast imaging (VCI)
  - Light-induced voltage alternation (LIVA)
  - Voltage alternation CIVA
- Effective, but expensive and time-consuming
- Require destructively using at least one sample chip
- Many ineffective for technologies in the nano-meter domain
- Not effective for randomly inserted Trojans

Trojan Detection: ATPG (Automatic Test Pattern Generation)

- Uses standard VLSI fault detection tools
- Applies a digital stimulus and inspects digital output of chip
- Digital stimulus is derived using the netlist of the chip
  - For parametric Trojans of the parametric type, the netlist of a chip is the same with and without the Trojan
- Likely to yield best results of parametric Trojans
  - Due to stealthy activation criteria
  - ATPG directed to generate tests for nodes and paths that are hard-to-detect (i.e., difficult to control and/or observe,)
- Not effective with functional Trojans
  - Trigger condition occurs with very low probability during functional testing
  - $1/2^{64}$ probability of getting detected during validation

Trojan Detection: Side Channel Analysis

- Effective in extracting information about internal operations of embedded devices
  - Timing, Power consumption, Electromagnetic emanation profiles
  - Differential Power, Electromagnetic (EM) Analysis
  - Average measurements from multiple samples to deal with noise problem
- Approach
  - Requires destruction of a few ICs to validate authenticity
  - Other ICs validated using side-channel analysis for absence of any significantly sized Trojans (3-4 orders of magnitude smaller than IC [2])
- Effective for detection of functional Trojans
  - Detects functional Trojans without activating them, i.e., through the measurement of their secondary action characteristics
  - Not effective for testing circuits at extremely low clock frequencies

Research Priorities and Security Requirements

Accurate Data Collection

- Accurate data is critical to secure chip manufacturing
  - Equipment availability decision
  - Integrity of the specifications of the manufactured product
  - Reliability and repeatability of the manufacturing process [5]
- Data integrity becomes more important with the adoption of the e-Manufacturing model
  - E.g. accurate readings of the process speed and cooling response rates, the process chamber status, calibration data, and sensor settings at the equipment controller level
- Accurate process data are critical to equipment setup, qualification, process control, and process monitoring.
- Data collection timeliness needed to support process control

Preventing/Detecting False Data Injection Attacks and Sensor Compromise

- Attacks possible through sensor compromise or by obtaining the secret key
- Preventing/detecting these attacks is critical.
- This requires the protection of the sensor readings and sensor software, eliminating message and data latency and ensuring accurate timestamps.
- Fault-tolerant time synchronization system using diverse time sources.

Trusted Recipe Management

- Trusted recipes are a critical security requirement
  - Trusted management of equipment configuration
  - Configuration changes can cause differences in process capability and outcomes
- Security measures to enforce trusted recipe management are needed
- Existing access control mechanisms do not meet the requirements of the industry
  - Equipment engineers with administrator privileges

Fine-Grained Access Control Management

- New fine-grained access control models to equipment and product recipes are needed
- Need to reduce the privilege over-entitlement problem
  - Allowing design, process, equipment, industrial and integration engineers to solve problems together,
  - Consider manufacturing line emergencies

A technician programs a product "Recipe" into an epi reactor.

Dynamic Patching

- Control systems are not typically suitable for frequent software patching and updates due to their high availability requirements.
- Software patches and updates are usually deployed on a fixed, calendar-based schedule
- Call to move to condition-based and predictive preventive maintenance .

Summary

Threats and Security Challenges in the Semiconductor Manufacturing Sector

- Threats
  - Threats to IT systems and networks
  - Threats to equipment sensors and controllers
- Attacks
  - Regular attacks
  - Targeted attacks
    - Process vs. final product
    - Sabotage vs. espionage
- Security Challenges
  - Equipment Control and Recipe Integrity
  - Process Data Integrity
  - Privilege Over-Entitlement

Conclusion

- Existing Hardware Trojan detection techniques not very effective
  - Detection during manufacturing may be more effective
  - Mask signatures
- Need to model the security implications of the physical interactions in semiconductor processing tools
- Need to consider security as part of system architecture and software development for
  - Semiconductor processing and measurement/metrology tools
    - Information flow and control paths have to be identified
    - Joint work between IC and tool manufacturing companies
  - Plant automation infrastructure

References

[1] S. Adee "The Hunt for the Kill Switch", IEEE Spectrum Vol. 45 Num. 5, pp 34-39, May 2008. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0

[2] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar. "Trojan detection using IC fingerprinting." Proceedings of the 28th IEEE Symposium on Security & Privacy, pp 296–310, May 2007.

[3] M. D. Dickey, K. J. Russell, D. J. Lipomi, V. Narayanamurty, and G. M. Whitesides. "Transistors Formed from a Single Lithography Step Using Information Encoded in Topography" - 2010 Wiley-VCH Verlag GmbH & Co. KGaA, Weinheim. http://www.small-journal.com.

[4] M. Hicks, M. Finnicum, S. King, M. Martin, and J. Smith. "Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically." Proceedings of the 31st IEEE Symposium on Security & Privacy, pp 159–172, May 2010.

References

[5] S. King, J. Tueck, A. Cozzie, C. Grier. W. Jiang, and Y. Zhou. “Designing and implementing malicious hardware.” Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pp 1-8, 2008.

[6] SEMATECH technical Publications. http://www.sematech.org/publications/technical.htm

[7] C. Sturton, M. Hicks, D. Wagner, and S. T. King. “Defeating UCI: Building Stealthy and Malicious Hardware.” Proceedings of the 32nd IEEE Symposium on Security & Privacy, pp 64-77, 2011.

[8] X. Wang and M. Tehranipoor. “Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions.” Proceedings of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, pp 15–19, 2008.

[9] A. Waskman and S. Sethumadhavan. “Tamper Evident Microprocessors”. Proceedings of the 31st IEEE Symposium on Security and Privacy, 2010.

References

[10] A. Waskman and S. Sethumadhavan. “Silencing Hardware Backdoors.” Proceedings of the 32nd IEEE Symposium on Security & Privacy, pp 49-63, 2011.

[11]“Dell warns of hardware trojan.” Homeland Security News Wire, July 2010. http://www.homelandsecuritynewswire.com/dell-warns-hardware-trojan

[12] J. Markoff. “F.B.I. Says the Military Had Bogus Computer Gear.” The New York Times, May 2008. http://www.nytimes.com/2008/05/09/technology/09cisco.html?_r=3&partner=rssnyt&emc=rss

Questions & Answers