Introduction

Mohammad Tehranipoor

ECE4095/6095: Introduction to Hardware Security & Trust
University of Connecticut
ECE Department

Acknowledgement

- Book Contributors
- Prof. Farinaz Joushanfar, Rice University
- Book:
  - M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011

ECE 4095/6095

- Title: "Hardware Security and Trust"
- Instructor
  - Mohammad Tehranipoor
- Meeting time
  - 12:45pm – 3:15pm Monday
- Meeting place
  - ITE 330
- Prerequisites
  - Self-contained, but assuming undergraduate level knowledge of digital logic design
  - An overview of VLSI design and test will be given

Overview

- Cryptographic cores:
  - Vulnerabilities, processing overhead
- Arracks:
  - Physical, invasive, non-invasine/side-channel
- Physically unclonable functions (PUFs), TRNG
- Anti-piracy:
  - Watermarking, passive and active metering
- FPGA security
  - Trusted design in FPGAs
- Hardware Trojan detection

Goals

- Learning the state-of-the-art security methods and devices as well as emerging technologies and security trends
- Integration of security as a design metric, not as an afterthought for the system
- Protection of the design intellectual property against piracy and tampering
- Better understanding of attacks and providing countermeasures against them
- Better understanding of vulnerabilities in design and fabrication processes and providing solution to prevent Trojan insertion and effectively detect them

Book and More…

- Reading
  - Papers from the contemporary literature
- Further possible reading
  - Mihir Bellare and Phil Rogaway, Introduction to Modern Cryptography
  - Ross J. Anderson, Security Engineering: A guide to building dependable distributed systems, John Wiley and Sons, 2001
  - Matt Bishop , Computer Security: Art and Science, Addison-Wesley, 2003
  - William Stallings, Cryptography and Network Security, Fourth edition, 2007
  - M. Tehranipoor and F. Koushanfar, "**A Survey of Hardware Trojan Taxonomy and Detection**," IEEE Design and Test of Computers, 2010.

Grading and Project

- Grading
  - Oral presentation (30%)
  - Exams (40%) (open book)
  - Class project (25%)
  - Class Participation (5%)
- Project
  - Groups of 1 or 2 (collaborations encouraged)
  - Either propose or select from my list of potential projects/datasets

Tools

- Hands-on experience with the FPGA testbed
  - Synthesis tools
- Statistical analysis of the attacks
  - R statistical computing package
- Tools:
  - Synopsys design flow

Course Outline (Cont'd)

1. Introduction to Hardware Security & Trust
2. Introduction to Cryptography
3. Basics of VLSI Design and Test
4. Security Based on Physically Unclonablability and Disorder
5. Hardware Metering
6. Watermarking of HW IPs
7. Physical Attacks and Tamper resistance
8. Side Channel Attacks and Countermeasures, Countermeasures for Embedded Microcontrollers
9. Fault Injection Attacks
10. Trusted Design in FPGAs
11. Security in Embedded Systems
12. Security for RFID Tags
13. Hardware Trojans: IC Trust (Taxonomy and Detection)
14. Hardware Trojans: IP Trust (Detection)
15. Design for Hardware Trust
16. Protecting against Scan-based Side Channel Attacks
17. Secure JTAG
18. Counterfeit Detection and Avoidance
19. Crypto Processor Design

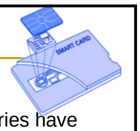
Course Outline (Cont'd)

- Each student will review literature for the selected topic, book chapter, and then prepare a set of slides to present the existing work.
- The slides will be prepared in close collaboration with the instructor
- The slides will be co-presented with the instructor
- Each student must write a complete report based on his/her study
- All students must use the same template for their presentation slides
- Class participation and Q&A is very important
- Final Exam will be based on all the topics covered by the instructor and students in the class
- Final project

Motivation – HW Security

- HW security is becoming increasingly popular,
  - **Hardware security sneaks into PCs,** Robert Lemos, CNET News.com, 3/16/05
  - **Microsoft reveals hardware security plans, concerns remain,** Robert Lemos, SecurityFocus 04/26/05
  - **Princeton Professor Finds No Hardware Security In E-Voting Machine,** Antone Gonsalves, InformationWeek 02/16/07
  - **Secure Chips for Gadgets Set to Soar,** John P. Mello Jr. TechNewsWorld, 05/16/07
  - **Army requires security hardware for all PCs**, Cheryl Gerber, FCW.com, 7/31/2006
  - Trust-hub.org

Time for smart cards



- By the end of 2006, Westerns European countries have fully migrated to smart cards
  - Voting: In Sweden you can vote with your smart card, which serves as a non-repudiation device
  - Telecommunications: Many cellular phones come with smart cards in Europe and will soon be shipping in the United States.
  - Mass Transit: British Air relies on rail and air connections more than most airports.
- In 2006, ~27M contactless cards were in circulation in US, the number is estimated to top 100M by 2011
  - E.g., homeland security has required the port workers to have smart ID cards (Jan, 2007)
  - Entertainment: Most DSS dishes in the U.S. have smart cards.

Smart Cards -- Attacks

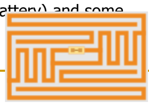
- Access Control: Smart Cards Under Attack - Literally, Ken Warren, Security Magazine, 03/17/2006
- Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks, Saar Drimer and Steven J. Murdoch, USENIX SECURITY, 2007
- Vulnerability Is Discovered In Security for Smart Cards, John Markoff, NY TIMES, 05/13/2002

RFIDs

Radio-frequency identification (**RFID**) is the use of an object (typically referred to as an RFID tag) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

Most RFID tags contain at least two parts:

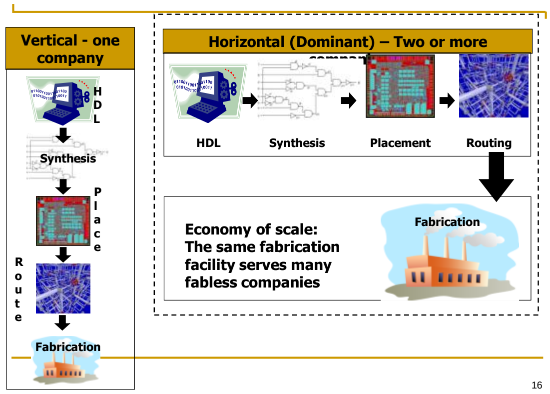
- An integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, and other specialized functions.
- An antenna for receiving and transmitting the signal.
- Some are active (battery) and some others are passive



RFIDs

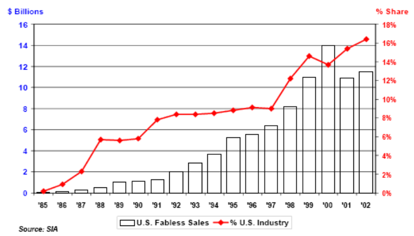
- Many applications in securing transactions,
  - Inventory Control Container / Pallet Tracking
  - ID Badges and Access Control
  - Fleet Maintenance Equipment/Personnel Tracking in Hospitals
  - Parking Lot Access and Control
  - Car Tracking in Rental Lots
  - Product Tracking through Manufacturing and Assembly
- Can we create security mechanisms light enough to be suitable for the RFIDs?

Shift in the Industry's Business Model



Microelectronic Industry Business Model

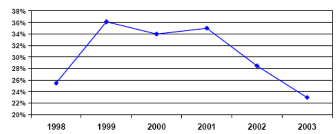
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry



Source: SIA

Leading-Edge Technology

U.S. industry's share of capital expenditures falling and in leading edge semiconductor manufacturing capacity.

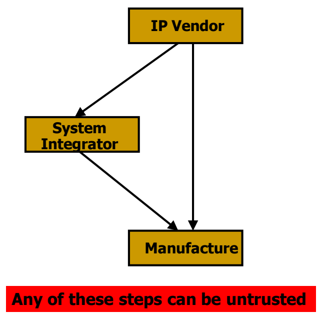


Leading Edge	< 0.4μ	< 0.3μ	< 0.3μ	< 0.2μ	< 0.2μ	< 0.16μ

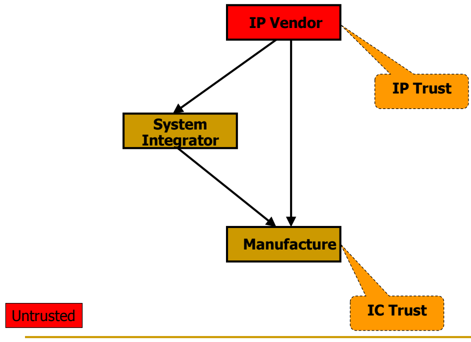
Source: SICAS/SIA

- The cost of building a full-scale, 300 mm wafer 65nm process chip fabrication plant is about $3bn

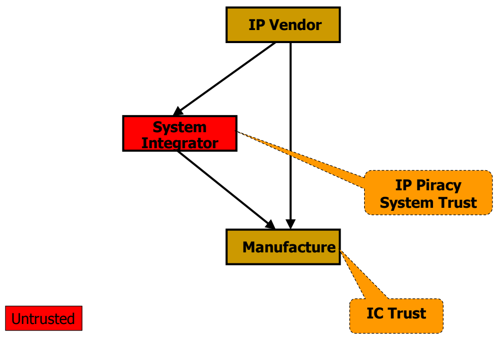
HW Threats



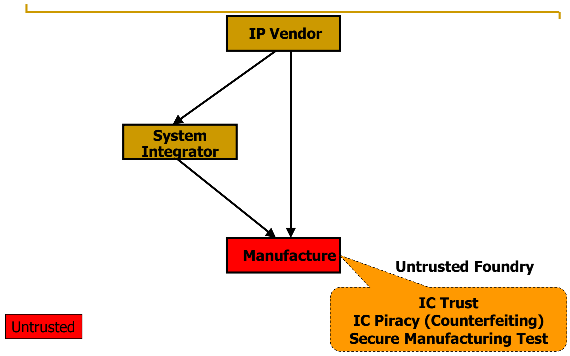
HW Threats



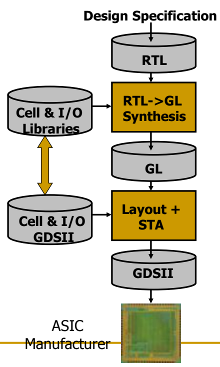
HW Threats



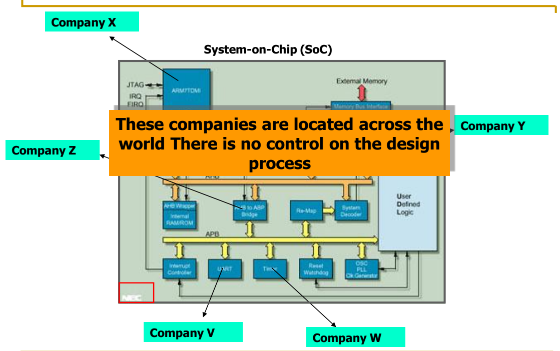
HW Threats



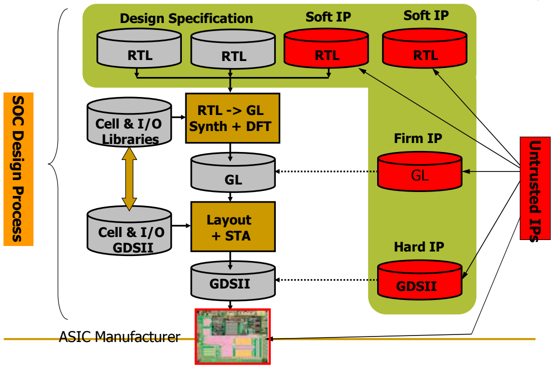
Design Process – Old Way



Issues with Third IP Design

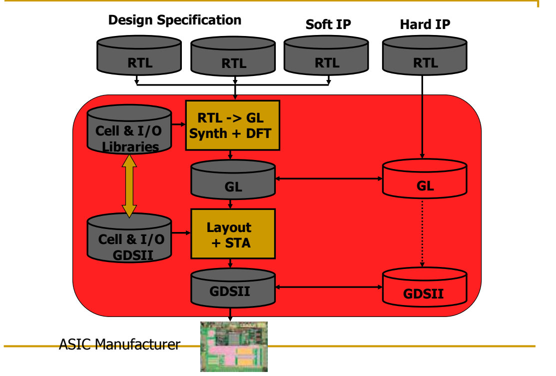


Design Process – New Way

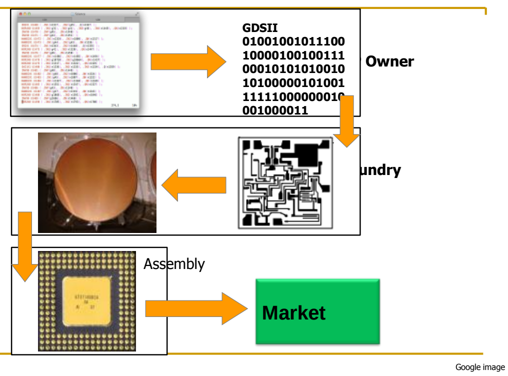


Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

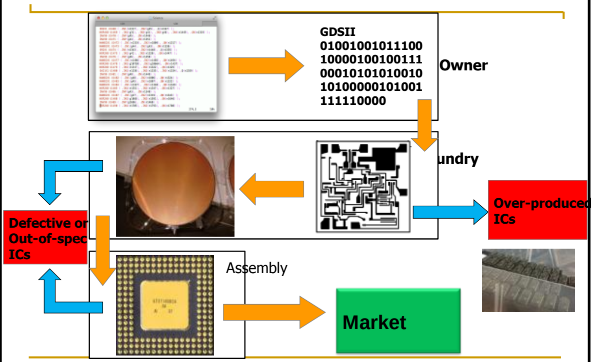
Untrusted System Integrator



Counterfeiting



Counterfeiting

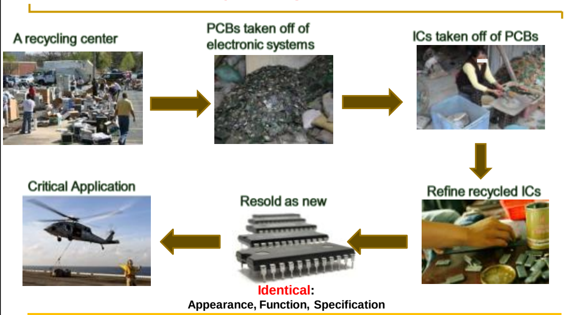


IC Counterfeiting

- Most prevalent attack today
- Unauthorized production of wafers
- It is estimated that counterfeiting is costing semiconductor industry more several billion dollars per year

Over production | Off-spec parts | Defective parts | Cloned ICs | Recycled ICs

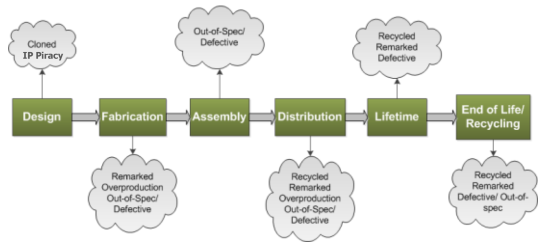
IC Recycling Process



Consumer trends suggest that more gadgets are used in much shorter time – more e-waste

Source: Images are taken from google

Supply Chain Vulnerabilities



Piracy – Some True Stories…

- In 2000, Chen Jin, finished Ph.D. in computer engineering at UT Austin
- He went back to China, first to Motorola research and then to Jiaotong University as a faculty
- In 2003, he supervised a team that created one of China's first homegrown DSP IC
- Chen was named one of China's brightest young scientists, funded his own lab, got a huge grant from the government
- In 2006, it was revealed that he faked the chip, stealing the design from Texas Instruments!
- Links to the article: 1, 2

The Athens Affair

- In March 8, 2005, Costas Tsalikidis, a 38-year-old Engineer working for Vodafone Greece committed suicide – linked to the scandal!
- The next day, the prime minister got notified that his cell phone – and those of many other high-rank officials – were hacked!
- Earlier in Jan, investigators had found rogue software installed on the Vodafone Greece by parties unknown
- The scheme did not depend on the wireless nature
- A breach in keeping keys in a file – Vodafone was fined €76 million December 2006!

Interesting Articles

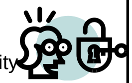
- The Hun for the Kill Switch, IEEE Spectrum, May 2008
- Find more interesting articles about hardware security and trust at: www.trust-hub.org

Some Basic Definitions

- **Intellectual property** represents the property of your mind or intellect - proprietary knowledge
- The four legally defined forms of IP
  - **Patents** When you register your invention with the government, you gain the legal right to exclude anyone else from manufacturing or marketing it
  - **Trademarks** A trademark is a name, phrase, sound or symbol used in association with services or products
  - **Copyrights** Copyright laws protect written or artistic expressions fixed in a tangible medium
  - **Trade secrets** A formula, pattern, device or compilation of data that grants the user an advantage over competitors

Some Basic Definitions (Cont'd)

- Cryptography:
  - crypto (secret) + graph (writing)
  - I like to call it the science of locks and keys
  - The keys and locks are mathematical
  - Underlying every security mechanism, there is a "secret"…
  - So the locks and keys are very useful in security
  - We are going to talk some about the traditional crypto, but we will also show new forms of security based on other forms of HW-based secret



Security and Protection Objectives, Attacks

Overview

- Definitions
  - What does secure mean?
  - Attacks
  - Computer security
  - Adversaries
  - Methods of defense
- Security in embedded systems, design challenges
- "Secret" -- root of cryptography

What Does Secure Mean?

- It has to do with an asset that has some value – think of what can be an asset!
- There is no static definition for "secure"
- Depends on what is that you are protecting your asset from
- Protection may be sophisticated and unsophisticated
- Typically, breach of one security makes the protection agent aware of its shortcoming

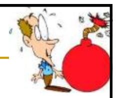
Typical Cycle in Securing a System

- Predict potential breaches
- Consider possible countermeasures, or controls
- Either actively pursue identifying a new breach, or wait for a breach to happen
- Identify the breach and work out a protected system again

Computer Security

- No matter how sophisticated the protection system is – simple breaches could break-in
- A computing system is a collection of hardware (HW), software (SW), storage media, data, and human interacting with them
- Security of SW, data, and communication
- HW security, is important and challenging
  - Manufactured ICs are obscure
  - HW is the platform running SW, storage and data
  - Tampering can be conducted at many levels
  - Easy to modify because of its physical nature

Definitions



- **Vulnerability**: Weakness in the secure system
- **Threat**: set of circumstances that has the potential to cause loss or harm
- **Attack**: The act of a human exploiting the vulnerability in the system
- Computer security aspects
  - **Confidentiality**: the related assets are only accessed by authorized parties
  - **Integrity**: the asset is only modified by authorized parties
  - **Availability**: the asset is accessible to authorized parties at appropriate times

Hardware Vulnerabilities

- Physical Attacks
- Trojan Horses
- IP Piracy
- IC Piracy & Counterfeiting
- Backdoors
- Non-tamper Resistant

Adversaries

- Individual, group or governments
  - Pirating the IPs – illegal use of IPs
  - Implementing Trojan horses
  - Reverse engineering of ICs
  - Spying by exploiting IC vulnerabilities
- System integrators
  - Pirating the IPs
- Fabrication facilities
  - Pirating the IPs
  - Pirating the ICs
- Counterfeiting Parties
  - Recycling, cloned, etc.

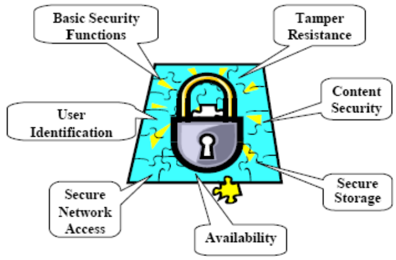
Hardware Controls

- Hardware implementations of encryption
  - Encryption has to do with scrambling to hide
- Design locks or physical locks limiting the access
- Devices to verify the user identities
- Hiding signatures in the design files
- Intrusion detection
- Hardware boards limiting memory access
- Tamper resistant
- Policies and procedures

Embedded Systems Security

- Security processing adds overhead
  - Performance and power
- Security is challenging in embedded systems
  - Size and power constraints, and operation in harsh environments
- Security processing may easily overwhelm the other aspects of the system
- Security has become a new design challenge that must be considered at the design time, along with other metrics, i.e., cost, power, area

Security Requirements



Secure Embedded Systems - Design Challenges

- Processing gap
- Battery gap
- Flexibility
  - Multiple security objectives
  - Interoperability in different environments
  - Security processing in different layers
- Tamper resistance
- Assurance gap
- Cost

Secret

- Underlying most security mechanism or protocol is the notion of a "secret"
  - Lock and keys
  - Passwords
  - Hidden signs and procedures
  - Physically hidden

"This is the secret of my success.
I delete everyone else's work."

Cryptography – History

- Has been around for 2000+ years
- In 513 B.C, Histiaeus of Miletus, shaved the slave's head, tattooed the message on it, let the hair grow

Cryptography – Pencil & Paper Era

- Caesar's cipher: shifting each letter of the alphabet by a fixed amount!
  - Easy to break
- Cryptoquote: simple substitution cipher, permutations of 26 letters
  - Using the dictionary and the frequencies, this is also easy to break

Cryptography – Mechanical Era

- Around 1900, people realized cryptography has math and stat roots
- German's started a project to create a mechanical device to encrypt messages
- Enigma machine → supposedly unbreakable
- A few polish mathematicians got a working copy
- The machine later sold to Britain, who hired 10,000 people to break the code!
- They did crack it! The German messages were transparent to enemies towards the end of war
  - Estimated that it cut the war length by about a year
- British kept it secret until the last working Enigma!

Cryptography – Mechanical Era

- Another German-invented code was Tunny
- Using a pseudorandom number generator, a seed produced a key stream ks
- The key stream xor'd with plain text p to produce cipher c: c=p⊕ks
- How was this code cracked by British cryptographers at Bletchley Park in Jan 1942?
- A lucky co-incidence!

Cryptography – Modern Era

- First major theoretical development in crypto after WWII was Shannon's Information Theory
- Shannon introduced the one-time pad and presented theoretical analysis of the code
- The modern era really started around 1970s
- The development was mainly driven by banks and military system requirements
- NIST developed a set of standards for the banks,
  - DES: Data Encryption Standard