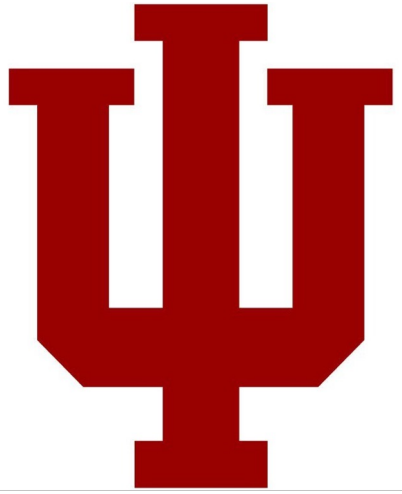
B590 → Canvas

Test

Introduction to Hardware Security

Engr 399/599: Hardware Security

Andrew Lukefahr
Indiana University



Adapted from: Mark Tehranipoor of University of Florida

What are you hoping to learn?

hardware vulnerabilities

mitigate vulnerabilities + explot

abstraction b/t HW & SW

TPM / Crypographic HW

cryptography

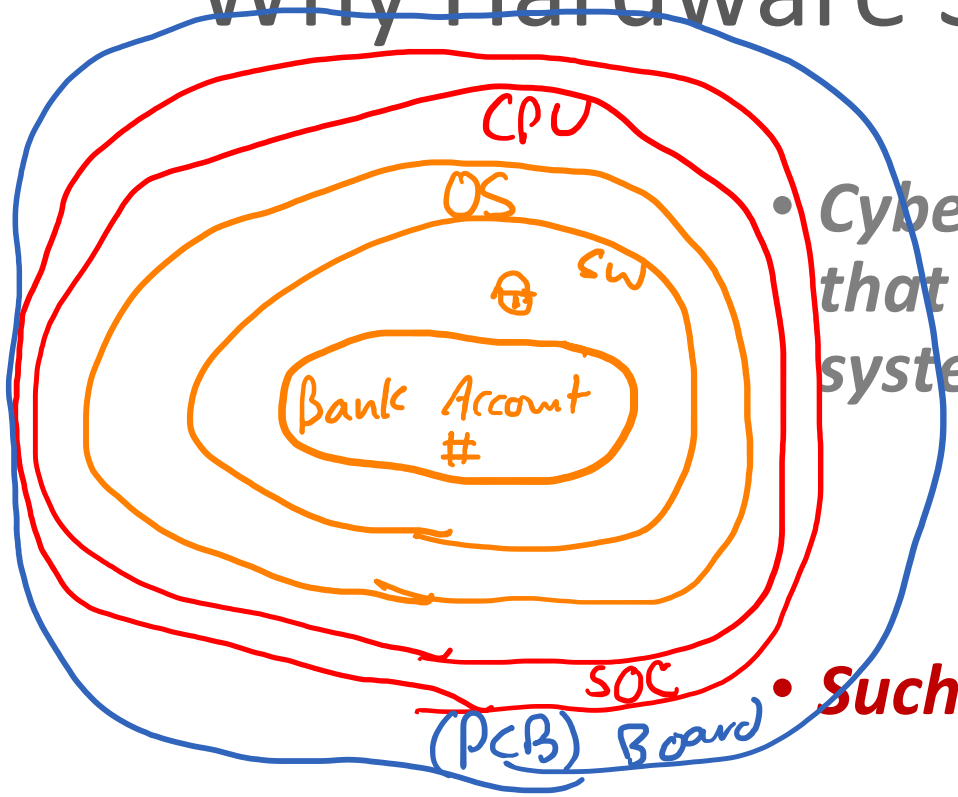
HW

Course Website

engr599.github.io

Write that down!

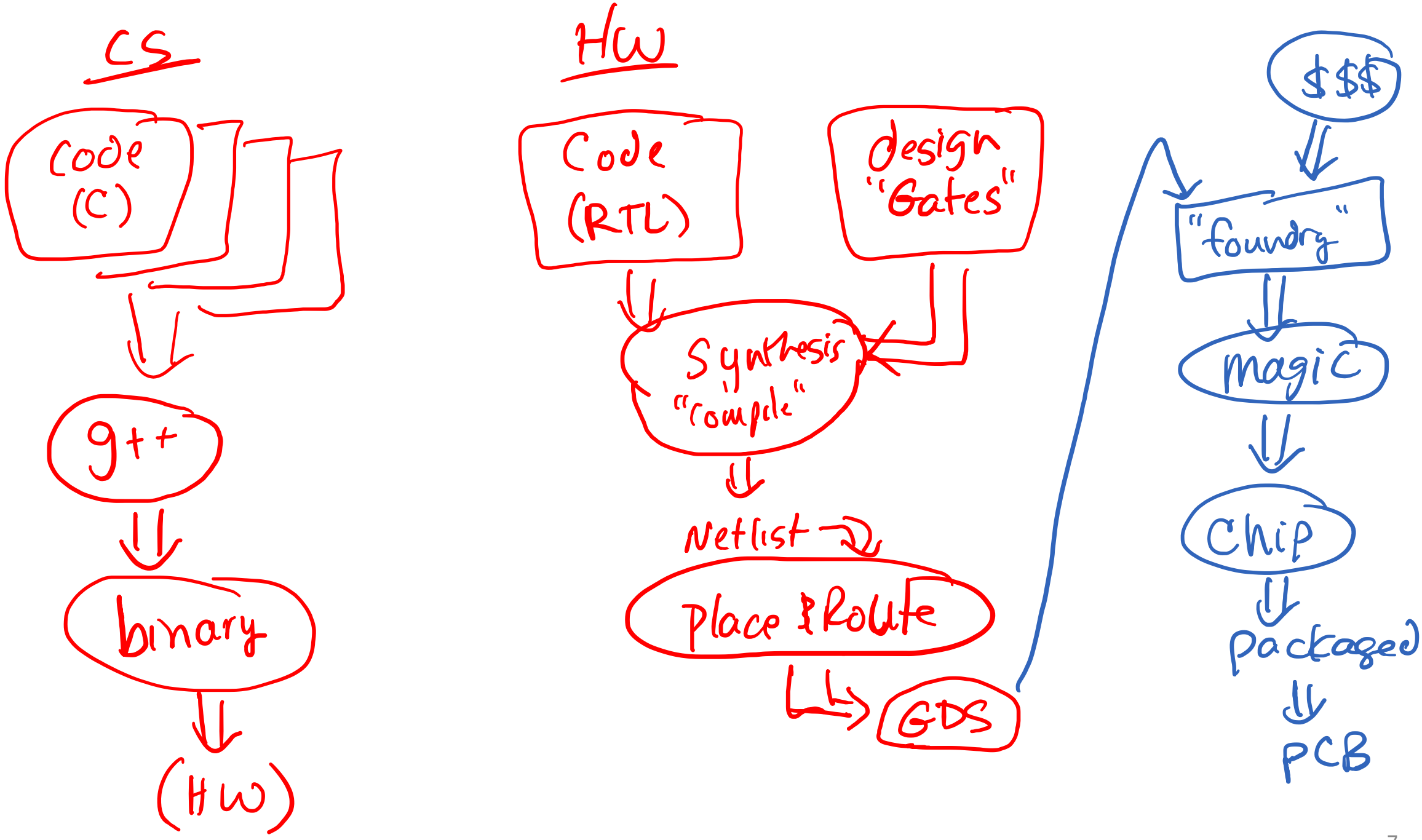
Why Hardware Security?



- *Cybersecurity experts have traditionally assumed that the hardware underlying information systems is secure and trusted.*
- ***Such assumptions are not true.***

The goals of this class are to:

- Learn the state-of-the-art security primitives and methods
- Integration of security as a design metric
- Protection of the design intellectual property against piracy and tampering
- Understanding of attacks and countermeasures
- Understanding of vulnerabilities in design and fabrication processes


CS
Code (C)
g++
binary
(HW)
HW
Code (RTL)
design "Gates"
Synthesis "compile"
Netlist
Place & Route
GDS
$$$
"foundry"
magic
Chip
packaged
PCB

Course Topics

- Hardware Security and Trust
- Hardware Cryptography
- Physically-Unclonable Functions (PUFs)
- True Random Number Generation (TRNG)
- Hardware Metering and Watermarking
- Hardware Physical and Fault-Injection Attacks
- Hardware Trojans
- Counterfeit Detection
- Side Channel Analysis
- FPGA Security
- PCB Security

About Me

Andrew Lukefahr, Assistant Professor

Office:	2032 Luddy Hall
Email:	*lukefahr@iu.edu*
Office Hours:	By Appointment

Research work on security and error resilience for FPGA-based systems.

About the TA: Barrett

Barrett Tieman

- Email: batieman@iu.edu

About You?

- Name
- Year / Department
- Why did you take this class?
- What are you hoping to learn?
- What's your background? Cybersecurity? Hardware?

Will
Sr ISE
HW

Owen
Sr ISE
HW

Alec
1st MS
Cyber

Anakil
Sr ISE
HW

Nicole
1 MS
HW

Joe
1st MS
Both

Vishal
2nd Yr sm
Cyber

Caleb
1st MS
HW / Cyber

Joe
Sr ISE
HW

Jason
Sr CS
-CS-

Jack
Sr CS
-CS-

Caleb
Sr ISE
Both

Brian
Sr ISE
HW

Ankit
2nd MS
Cyber

Adewale
2nd MS ISE
HW

Dave
1st PHD
HW

Jason
1st MS
Cyber

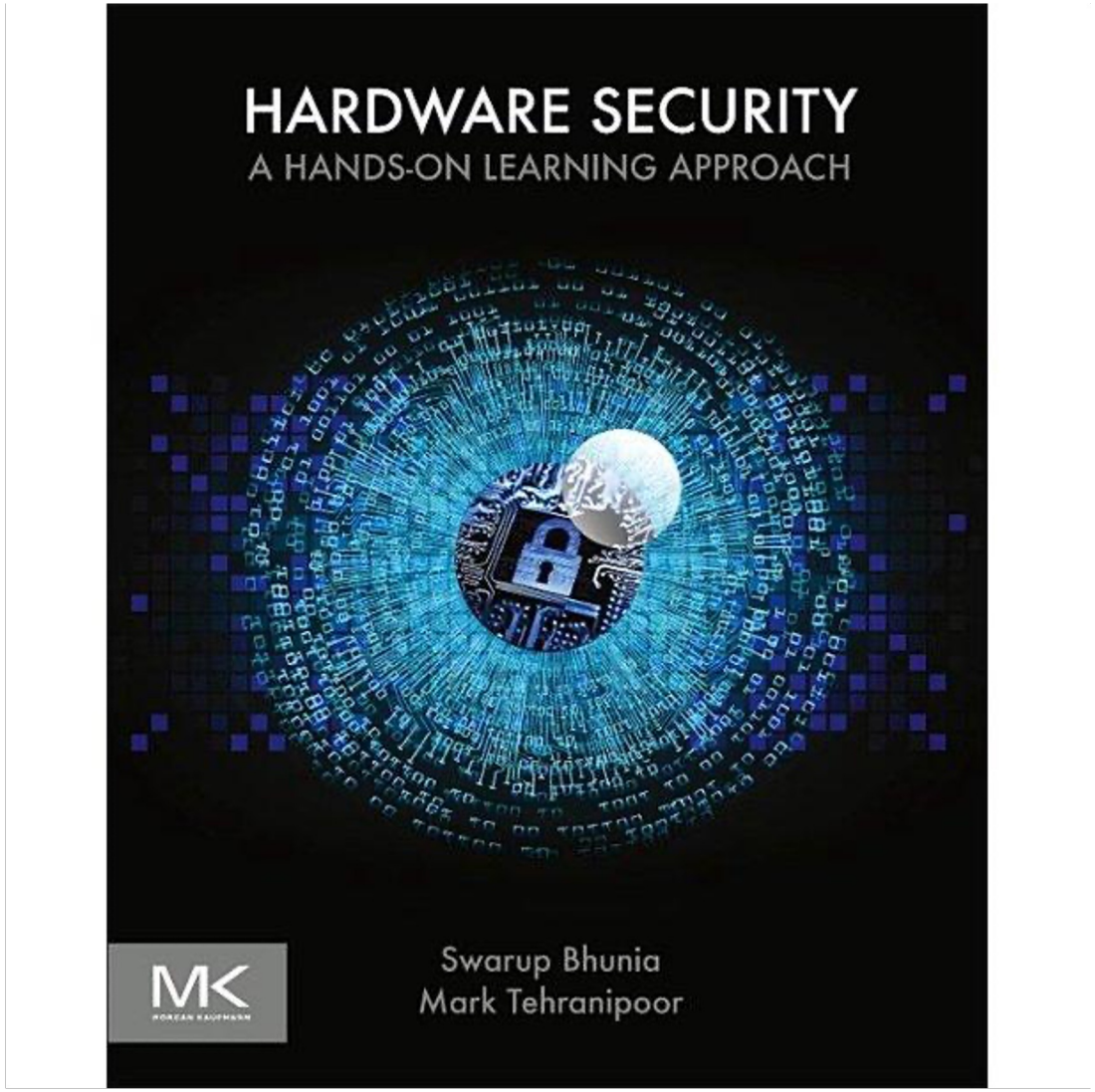
Joey
CS, Sr
Cyber

Omair
Sr ISE
HW

Nicky
Jr ISE
HW

Kaushik
1st MS
both

12 HW
9 SW



- Available online through IU's Library (See syllabus)

Grading

- The syllabus currently says this:

Exams	Projects	Participation
25%	40%	10%

Floating 25%

- This might change. We're still working out the projects.

A note on the slides

- These slides are adapted from an equivalent course at the University of Florida
- They are dense
- Please stop me and ask questions

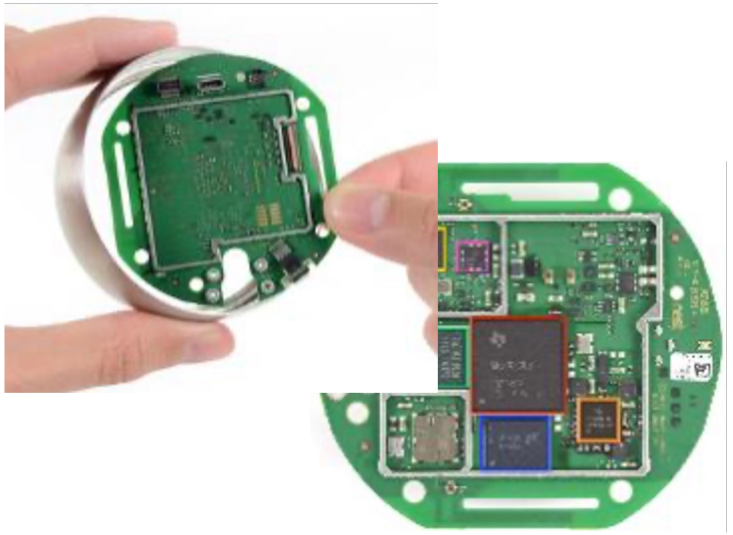
More to Read …

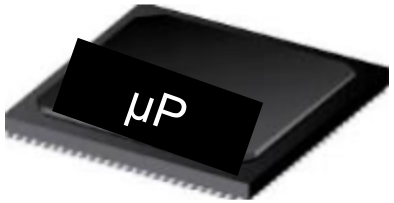
- **Reading**
  - Papers from the contemporary literature
- Further possible reading
  - Mihir Bellare and Phil Rogaway, **Introduction to Modern Cryptography**
  - Ross J. Anderson. **Security Engineering: A guide to building dependable distributed systems**. John Wiley and Sons, 2001
  - Matt Bishop, **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.
  - M. Tehranipoor, H. Salmani, and X. Zhang, **Integrated Circuit Authentication: Hardware Trojans and Counterfeit Detection**, Springer July 2013.
  - U. Guin, D. DiMase, and M. Tehranipoor, "**Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead**," Journal of Electronic Testing: Theory and Applications (**JETTA**), Feb. 2014.

More to Watch!

- **Videos**
  - What's inside a microchip? http://www.youtube.com/watch?v=GdqbLmdKgw4
  - Zoom Into a Microchip http://www.youtube.com/watch?v=Fxv3JoS1uY8
  - Public Key Cryptography: RSA Encryption: http://www.youtube.com/watch?v=wXB-V_Keiu8
  - Counterfeit Electronics Could Be Dangerous, Funding Nefarious People http://www.youtube.com/watch?v=dbZiUe6guxc
  - How Computers and Electronics Are Recycled http://www.youtube.com/watch?v=lw4g6H7alvo
  - Counterfeit Electronic Components Process http://www.youtube.com/watch?v=5vN_7NJ4qYA
  - Counterfeit Inspection http://www.youtube.com/watch?v=MbQUvu2LN6o
  - Gold from waste circuit electronics http://www.youtube.com/watch?v=ZkhOuNvkuu8
  - Tarnovsky Deconstruct Processor https://www.youtube.com/watch?v=w7PT0nrK2BE

What is Hardware?





- Electronic System
- System Hardware – acts as the ***"root-of-trust"***: PCB → IC (SoC | µP)

What is a “Root-of-Trust”?

Example Attack

Roy Zoppoth stands over a Xerox 914 copy machine, the world's first, which was used in soviet embassies all over the world. The machine was so complex that the CIA used a tiny camera designed by Zoppoth to capture documents copied on the machine by the soviets and retrieved them using a "Xerox repairman" right under the eyes of soviet security.

Photo from edit international courtesy of Roy Zoppoth

Motivation – HW Security

- **HW security is becoming increasingly important**
  - 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
  - Visit Facebook group on Hardware Security

Example Attack

Pentagon’s ‘Kill Switch': Urban Myth?

The Pentagon is worried that "backdoors" in computer processors might leave the American military vulnerable to an instant electronic shut-down. Those fears only grew, after an Israeli strike on an alleged nuclear facility in Syria. Many speculated that Syrian air defenses had been sabotaged by chips with a built-in ‘kill switch" — commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar."

This all had a very familiar ring to it. Those with long memories may also recall exactly the same scenario before: air defenses knocked out by the secret activation of code smuggled though in commercial hardware.

This was back in 1991 and the first Iraq War, when the knockout blow was administered by a virus carried by a printer : One printer, one virus, one disabled Iraqi air defense.

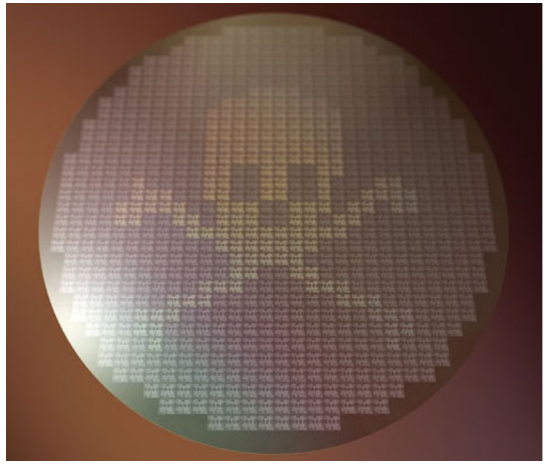
Example Attack

DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools

- Top homeland securities have admitted instances where along with software, hardware components that are being imported from foreign parties and used in different US systems are being compromised and altered to enable easier cyber-attacks.

The Hunt for Kill Switch, IEEE Spectrum 2008

- Increasing threat to hardware due to globalization
- Extremely difficult to detect kill switches (utilized by enemies to damage/destroy opponent artillery during critical missions) as well as intentional backdoors (to enable remote control of chips without user knowledge), which may have huge consequences
- Example: Syrian's Radar during Israeli attack, French Government using kill switches intentionally as a form of active defense to damage the chips if they fall in hostile hands, and more...



Example Attack

Fake Cisco routers risk "IT subversion”

- An internal Federal Bureau of Investigation presentation states that counterfeit Cisco routers imported from China may cause unexpected failures in American networks. The equipment could also leave secure systems open to attack through hidden backdoors.
- $76 million **fake Cisco routers**

Energy Theft Going From Bad to Worse

- Tampering with “smart” meters
  - Oil, electricity, gas, …
- $1B loss in CT because of electricity theft

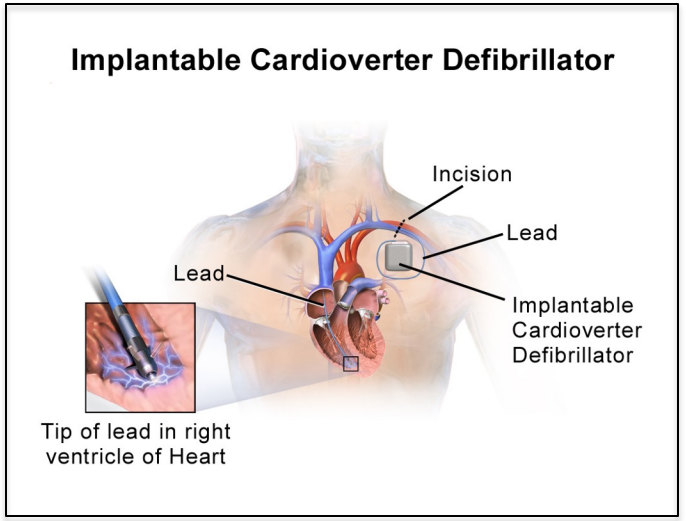
Example Attack

The deadly world of fake medicine – CNN.com

- A **counterfeit medication** or a counterfeit drug is a medication or pharmaceutical product which is produced and sold with the intent to deceptively represent its origin, authenticity or effectiveness.

Medical Device Security

- Incorporating security is sometimes considered expensive
- Implantable devices: e.g., Heart rate monitor
  - Incorporating Security could potentially reduce the life-time of the device by 30%
  - Attacking these device could result in loss of lives



Example Attack

Physical Attacks on Chip IDs

- Extracting secret keys

Side-Channel Attacks

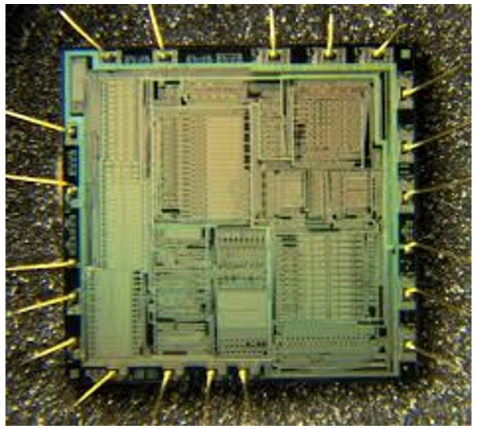
- Power Analysis, Timing Analysis, EM Analysis

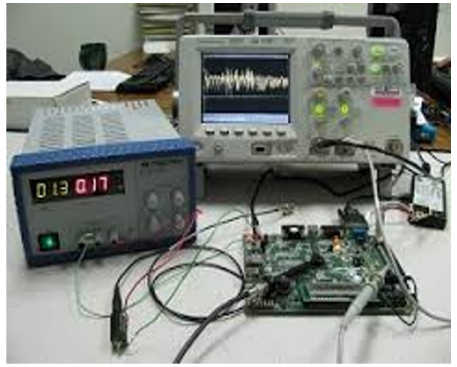
Tampering with Electronic Devices

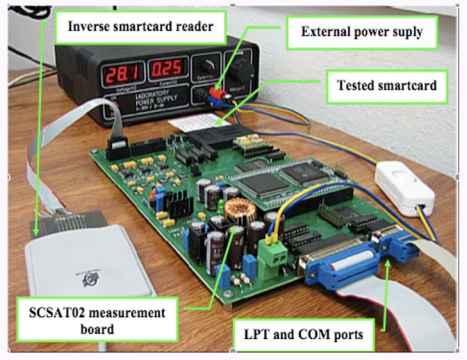
- Captured Drone by Iran

Counterfeit Integrated Circuits

- Multi-billion dollar business







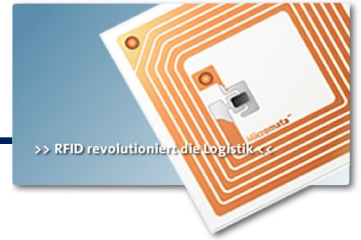
Time for Smart Cards

- By the end of 2006, Westerns European countries 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 (Digital Satellite Service) 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

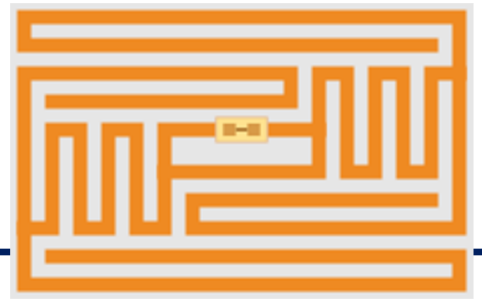
RFIDs



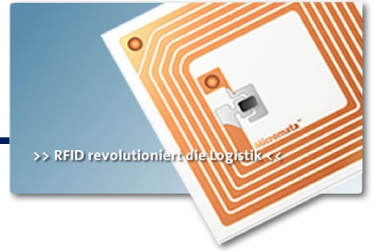
Radio-frequency identification (**RFID**) is the use of an object (typically referred to as an RFID tag) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

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
- Challenge: Can we create security mechanisms light enough to be suitable for the RFIDs?

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 Hunt for the Kill Switch**, IEEE Spectrum, May 2008
- J. Villasenor and M. Tehranipoor, "**The Hidden Dangers of Chop Shop Electronics**" IEEE Spectrum, Sep. 2013.
- M. Tehranipoor, U. Guin, and S. Bhunia, "**Invasion of the Hardware Snatchers: Fake Hardware Could Open the Door to Malicious Malware and Critical Failure**," IEEE Spectrum, 2017.
- S. Quadir, J. Chen, D. Forte, N. Asadi, S. Shahbaz, L. Wang, J. Chandy, and M. Tehranipoor, "**A Survey on Chip to System Reverse Engineering**," ACM Journal on Emerging Technologies in Computing Systems (JETC), 2015.
- M. Alam, M. Tehranipoor, and U. Guin, "**TSensors Vision, Infrastructure, and Security Challenges in Trillion Sensor Era**," Journal of Hardware and Systems Security (HaSS), 2017.
- K. Yang, H. Shen, D. Forte, S. Bhunia, and M. Tehranipoor, "**Hardware-Enabled Pharmaceutical Supply Chain Security**," ACM Transactions on Design Automation of Electronic Systems (TODAES), 2017.
- F. Rahman, B. Shakya, X. Xu, D. Forte, and M. Tehranipoor, "**Security Beyond CMOS: Fundamentals, Applications, and Roadmap**," IEEE Transactions on VLSI (TVLSI), 2017.


Meltdown


Spectre

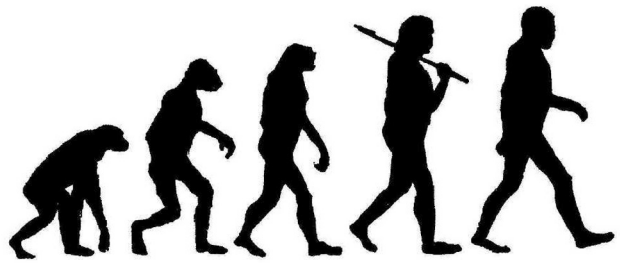
Apple zero-click iMessage exploit used to infect iPhones with spyware

By **Sergiu Gatlan**

September 7, 2023 04:18 PM 0

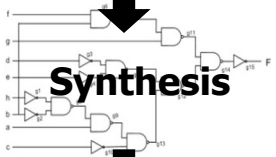
Evolution of Hardware Security and Trust

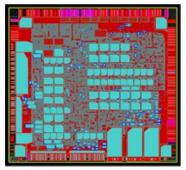
- **Prior to 1996:** Coating, encapsulation, labeling, taping, … still many companies don't spend much for securing their hardware
- **1996**: Extracting secret keys using power analysis – started the side-channel signal analysis era
- **1998**: Hardware unique ID
- **2002**: Physically Unclonable Functions (PUFs), True Random Number Generation (TRNG), Hardware tagging
- **2004-2007**: DARPA TRUST, Hardware trust
- **2008:** DARPA IRIS Program – Reverse engineering, tampering, and reliability
- **2008**: Counterfeit ICs
- **2012**: Senate Armed Services – National Defense Authorization Act (NDAA) 2012
- **2014**: DARPA SHIELD – Supply chain security
- **2015**: DARPA LADS
- More…



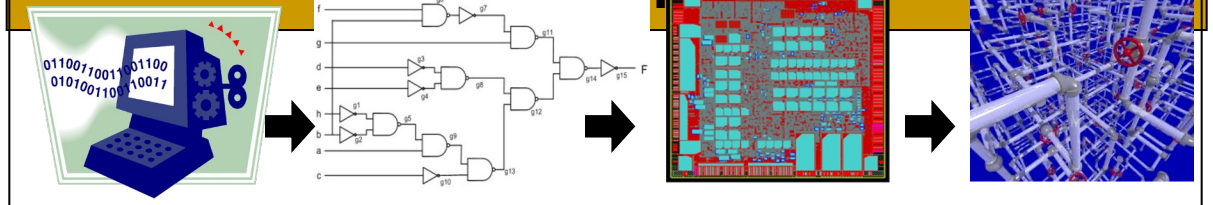
Shift in the Industry's Business Model

Vertical - one company





Horizontal (Dominant) – Two or more companies

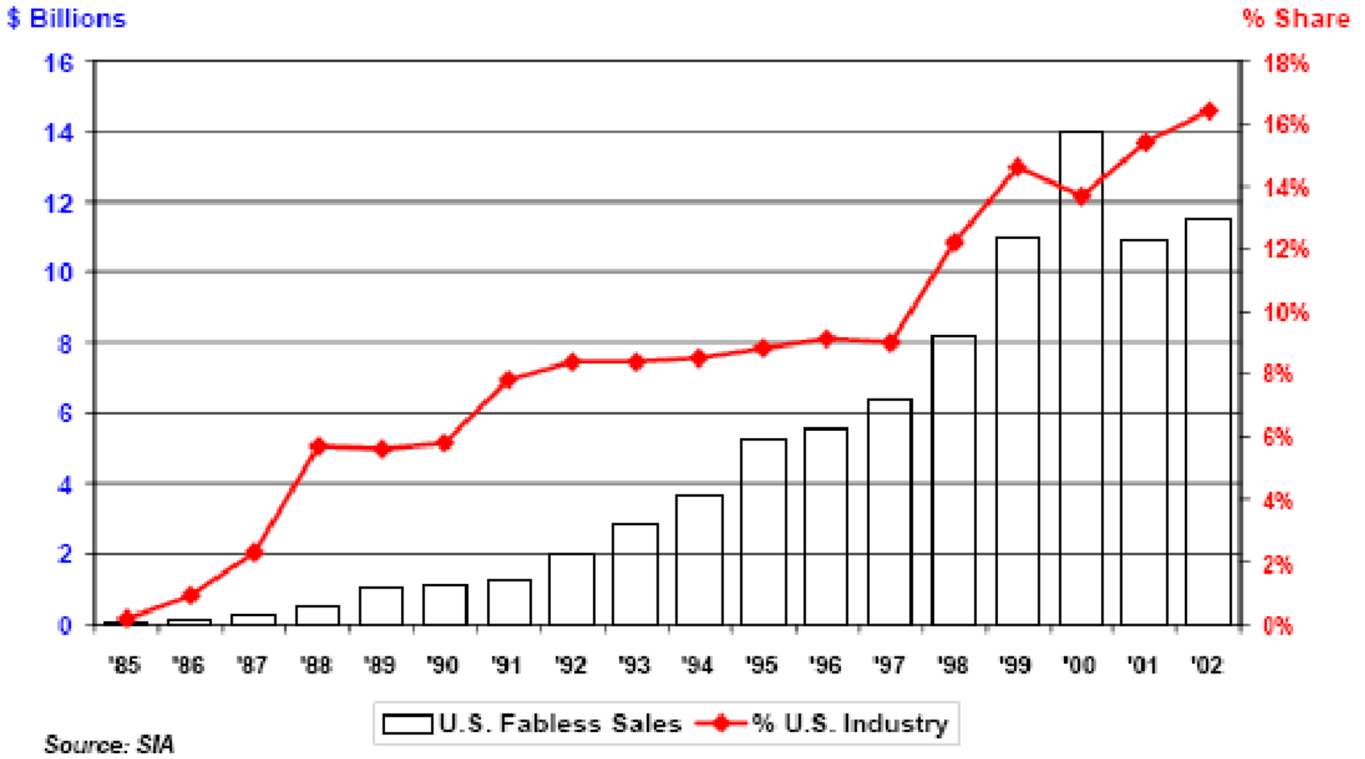


Economy of scale:
The same fabrication facility serves many fabless companies

stop here

Microelectronic Industry Business Model

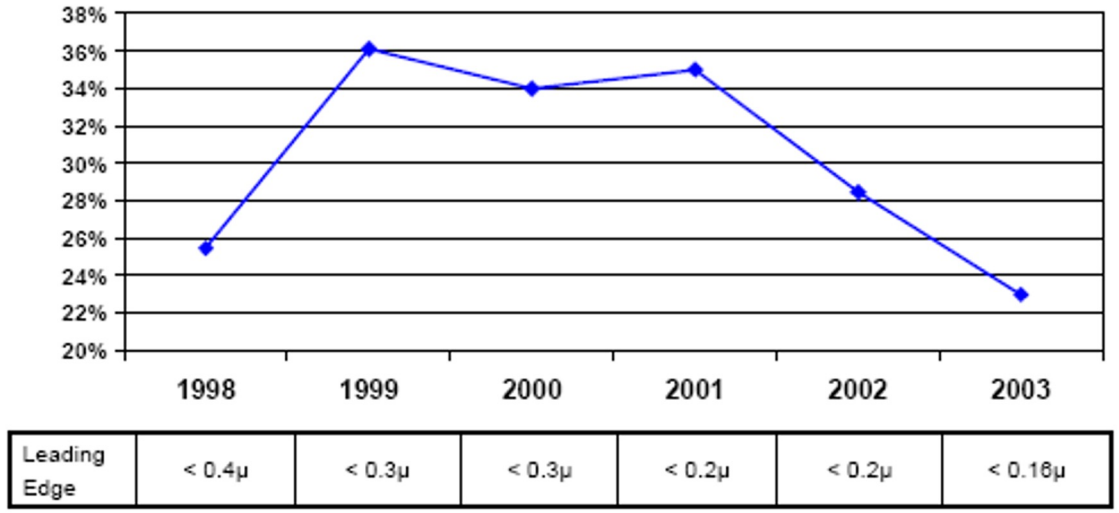
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry



Source: SIA

Leading-Edge Technology

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

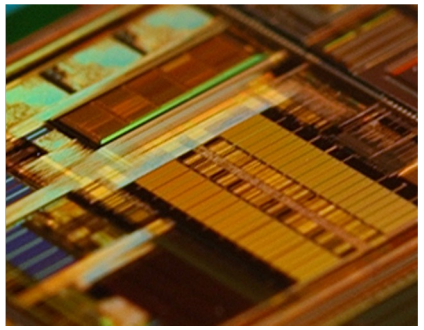


Leading Edge	< 0.4µ	< 0.3µ	< 0.3µ	< 0.2µ	< 0.2µ	< 0.16µ

Source: SICAS/SIA

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

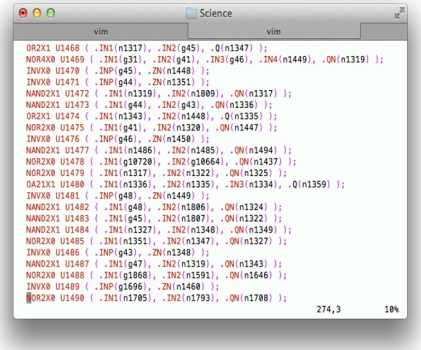
HW Threats



IP Vendor

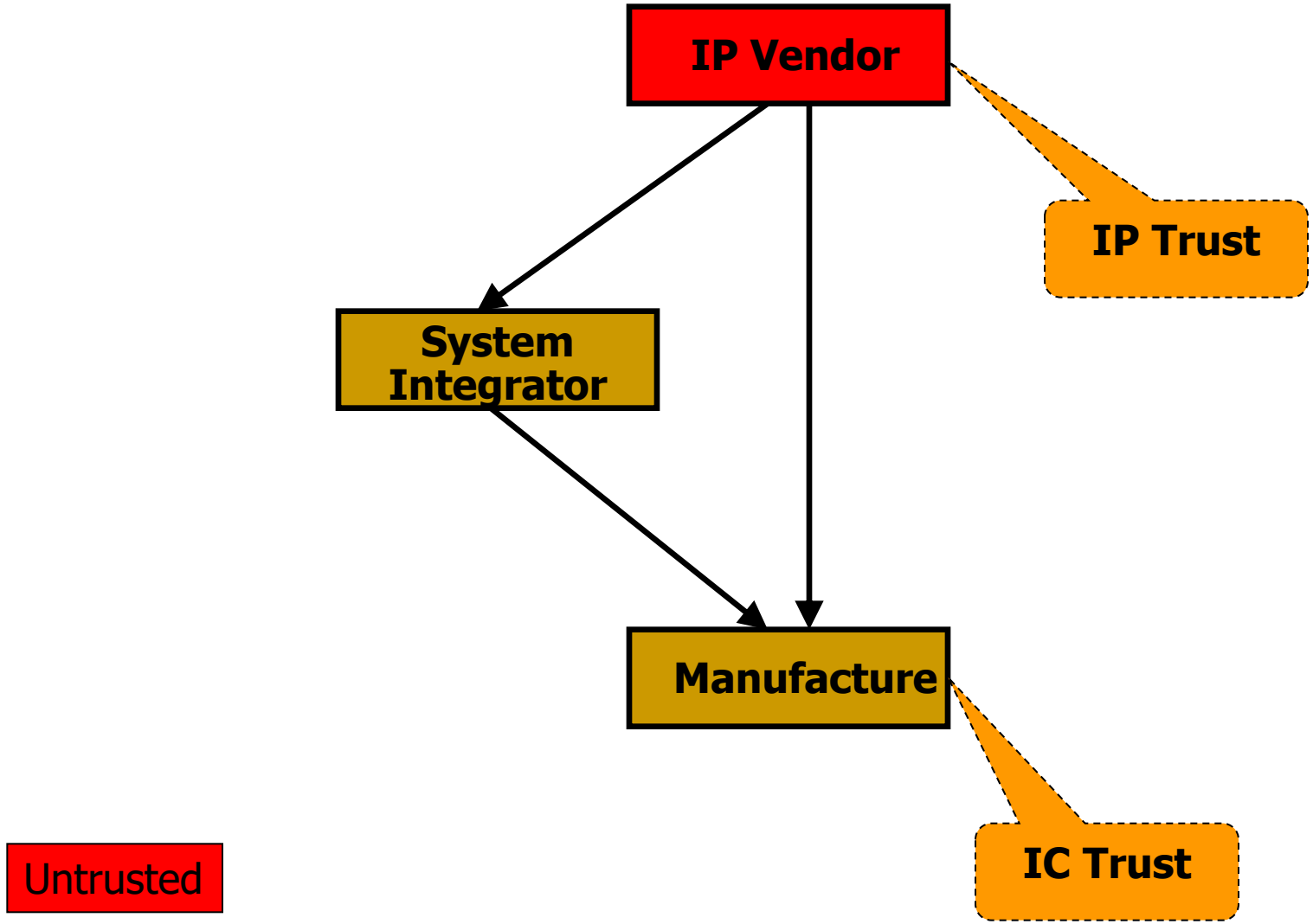
System Integrator

Manufacturer

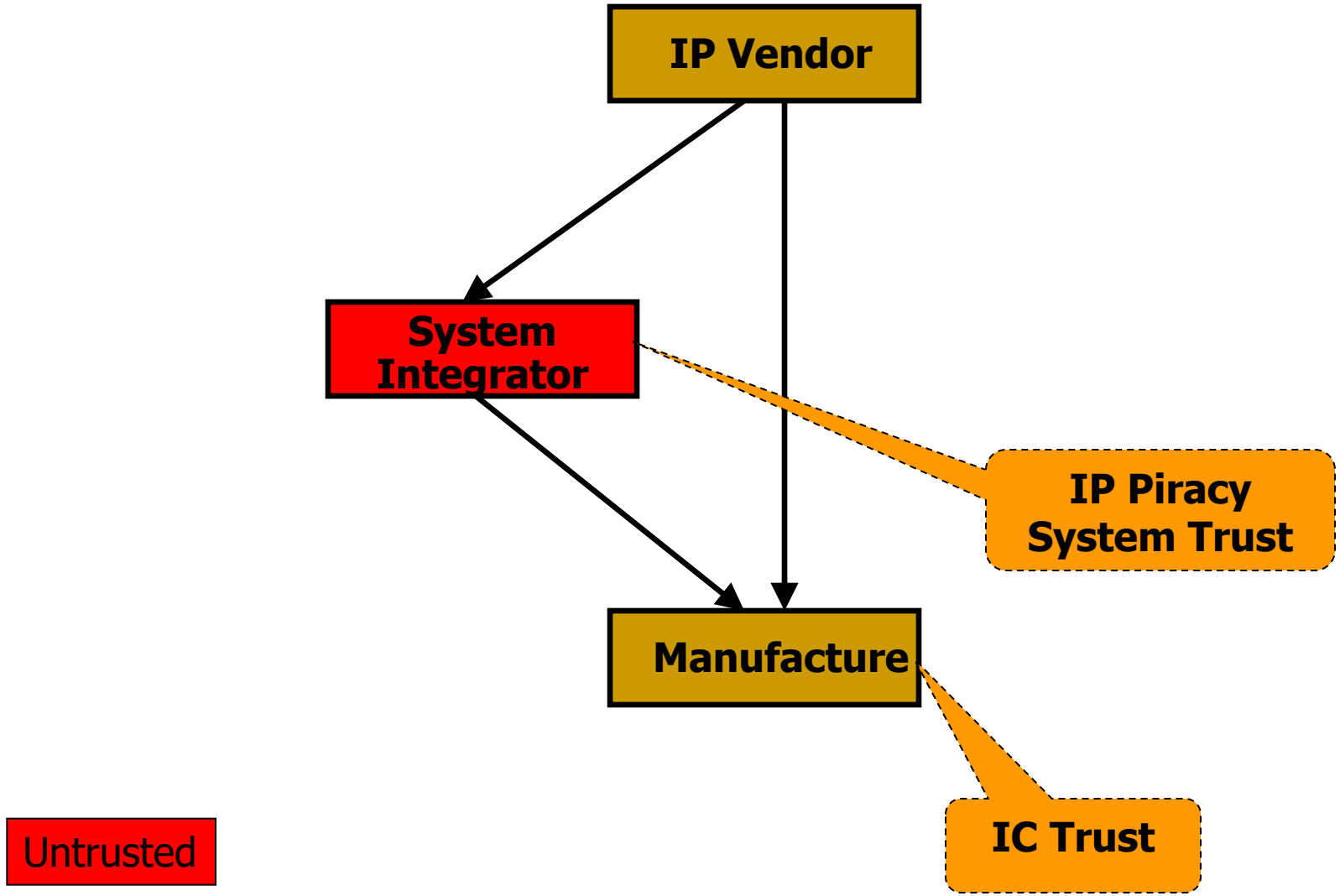


Any of these steps can be untrusted

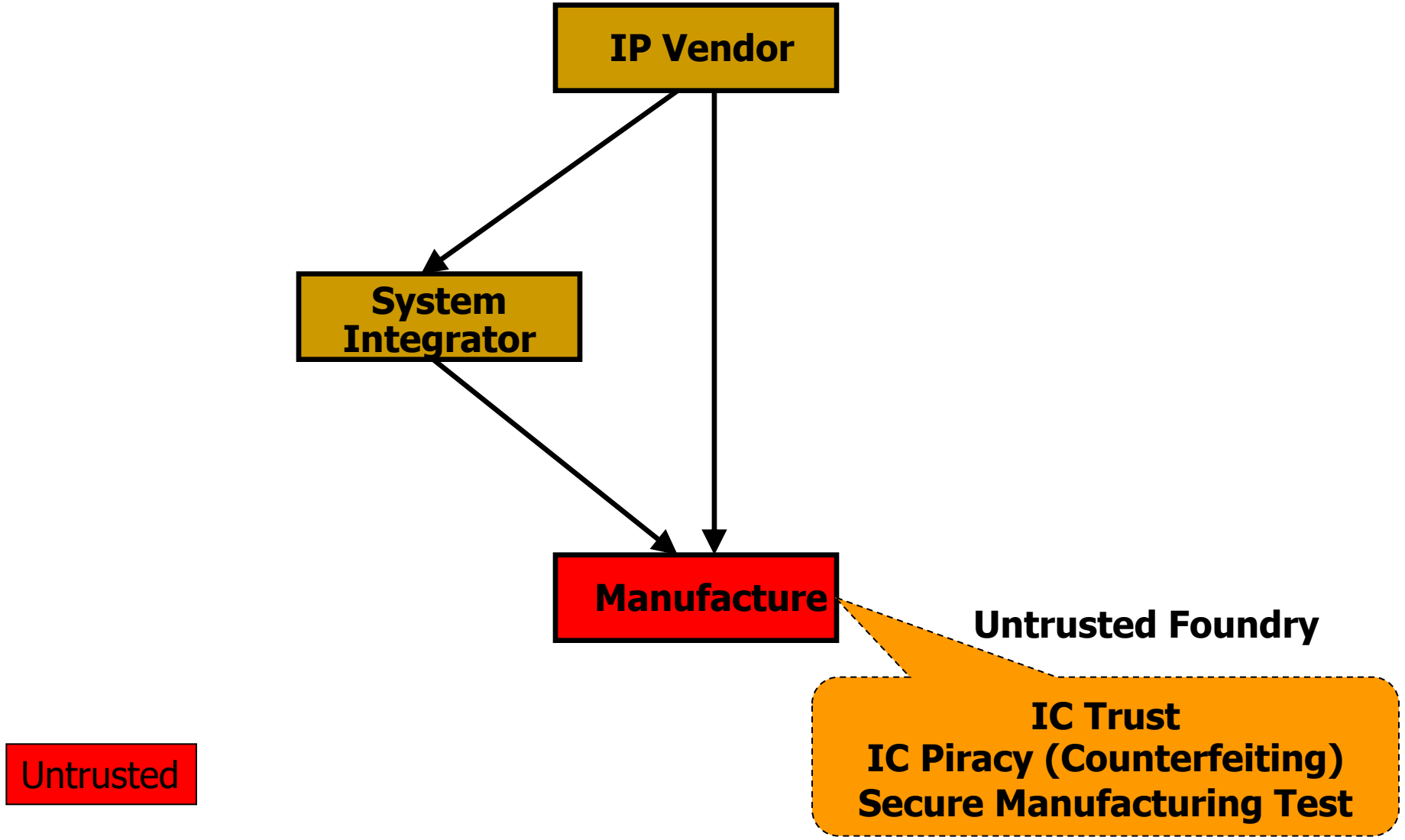
HW Threats


IP Vendor
IP Trust
System Integrator
Manufacture
IC Trust
Untrusted

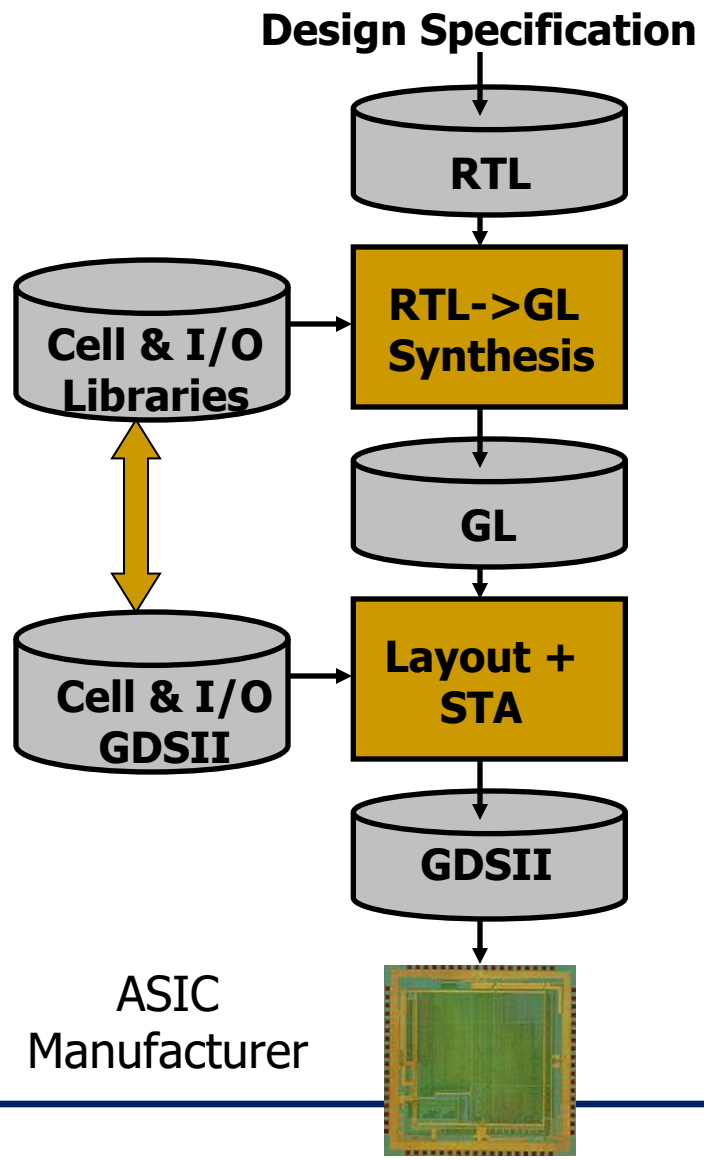
HW Threats


IP Vendor
System Integrator
IP Piracy
System Trust
Manufacture
IC Trust
Untrusted

HW Threats

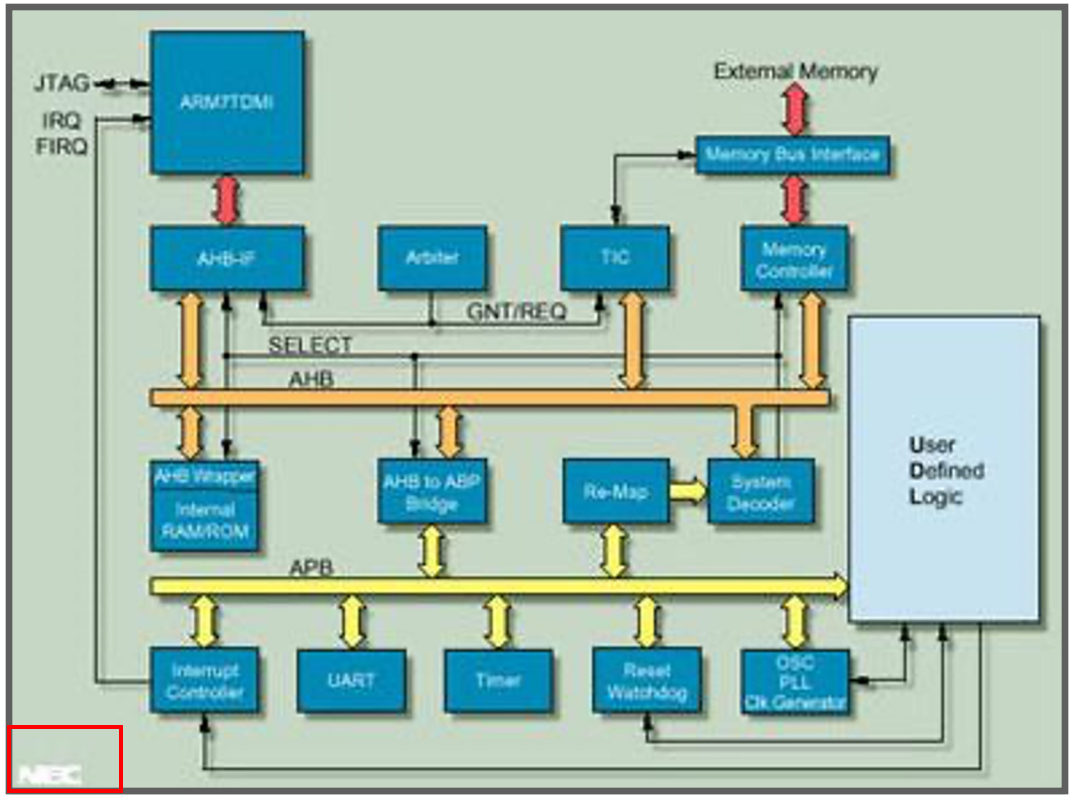

IP Vendor
System Integrator
Manufacture
Untrusted Foundry
IC Trust
IC Piracy (Counterfeiting)
Secure Manufacturing Test
Untrusted

Design Process – Old Way

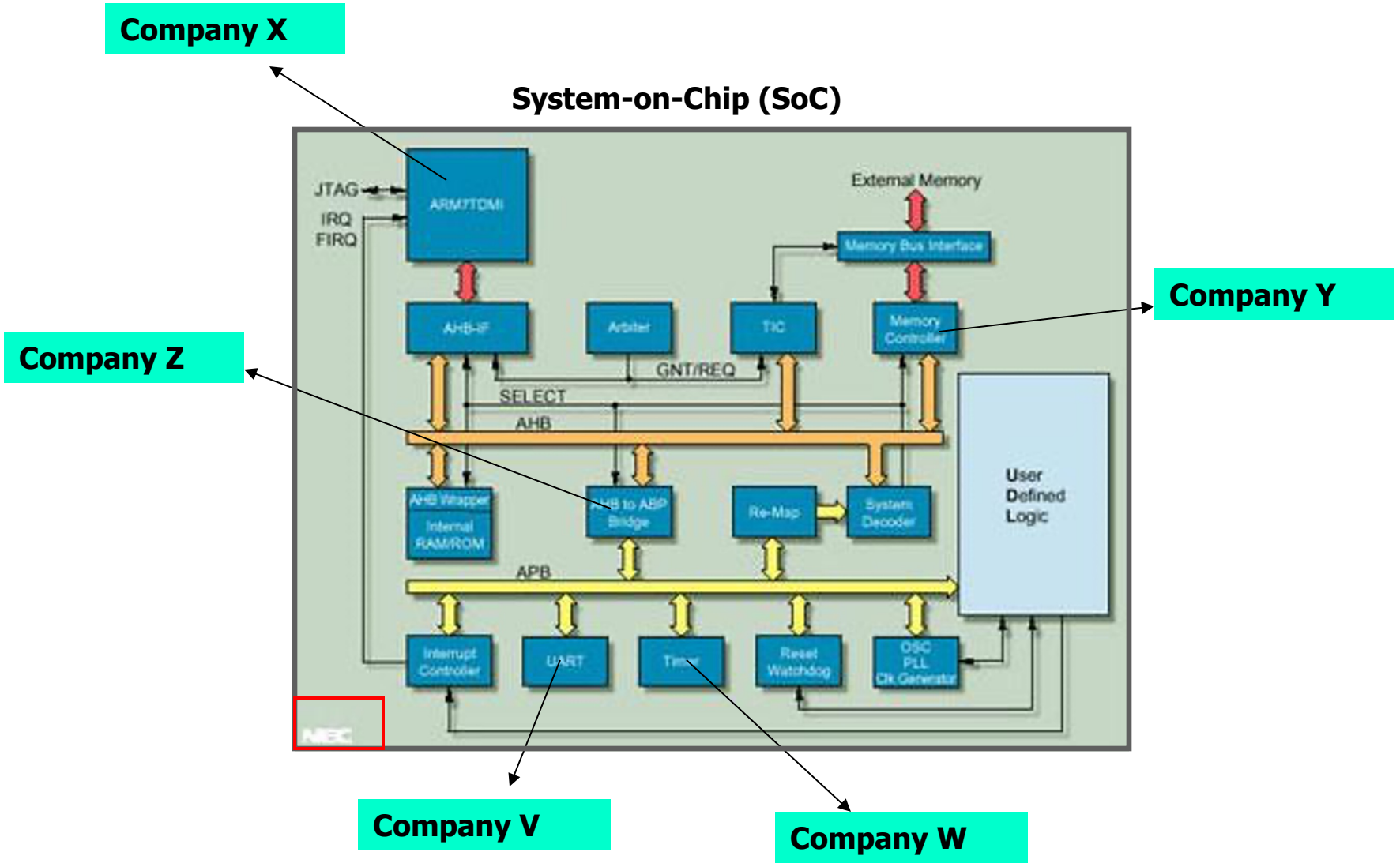


Issues with Third-Party IP Design

System-on-Chip (SoC)



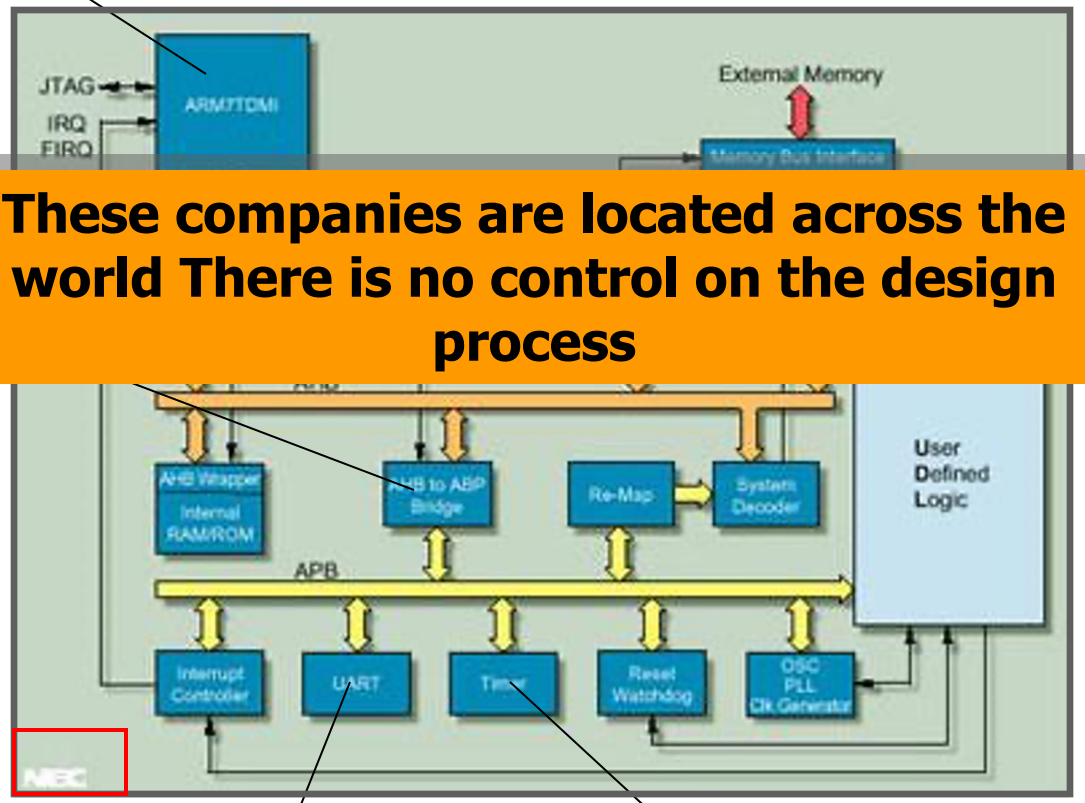
Issues with Third-Party IP Design



Issues with Third-Party IP Design

Company X

System-on-Chip (SoC)



These companies are located across the world There is no control on the design process

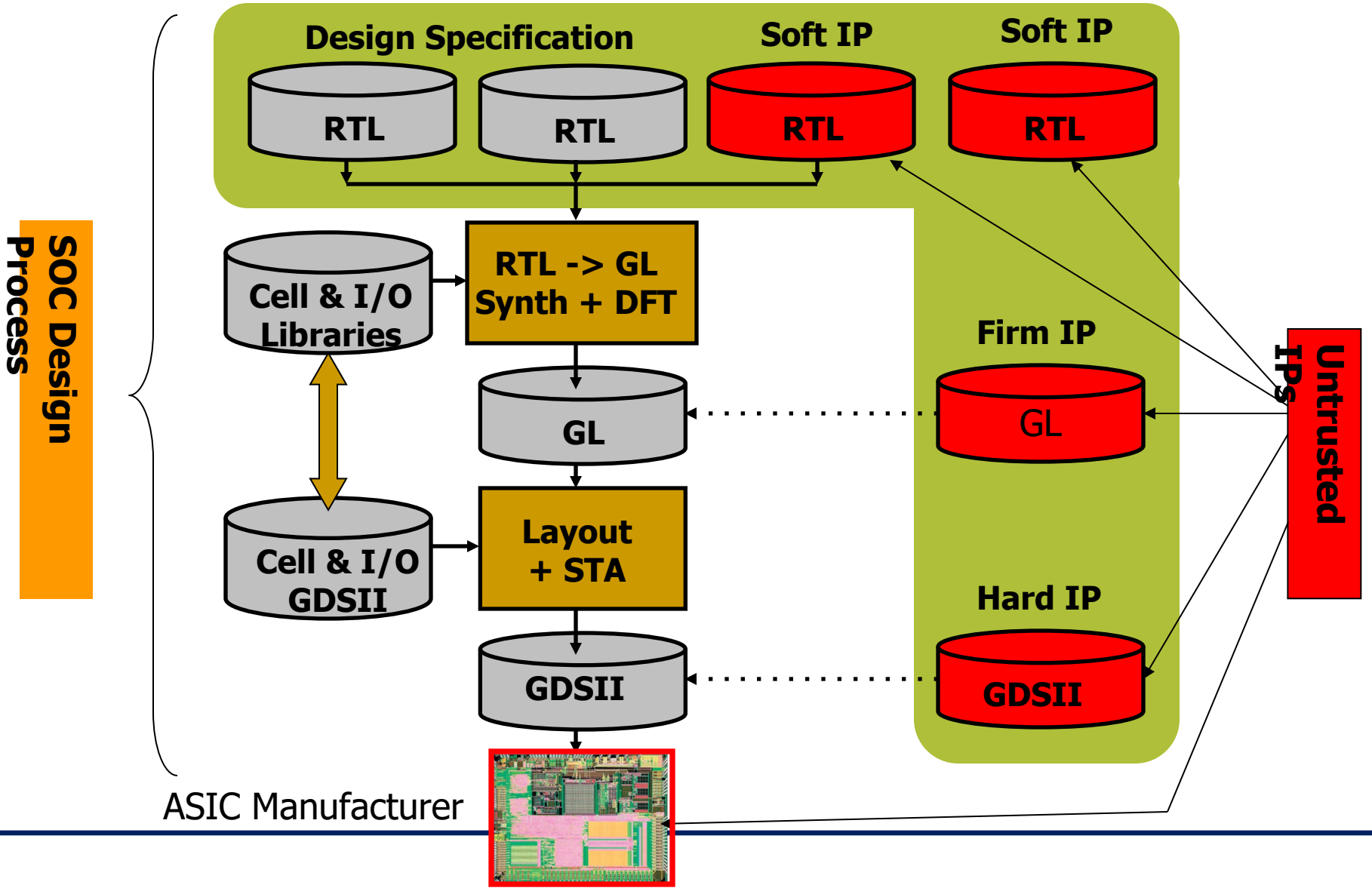
Company Y

Company Z

Company V

Company W

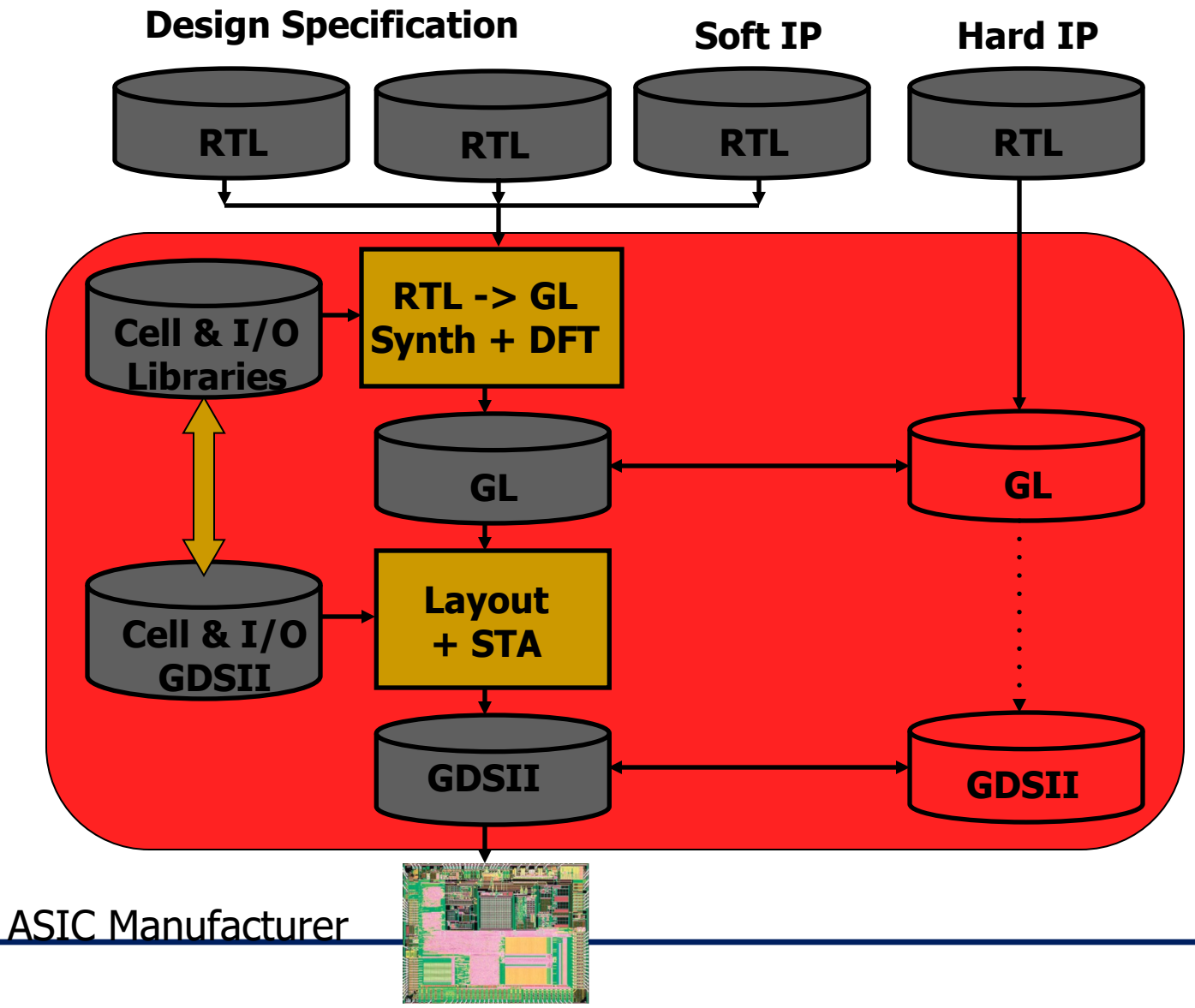
Design Process – New Way



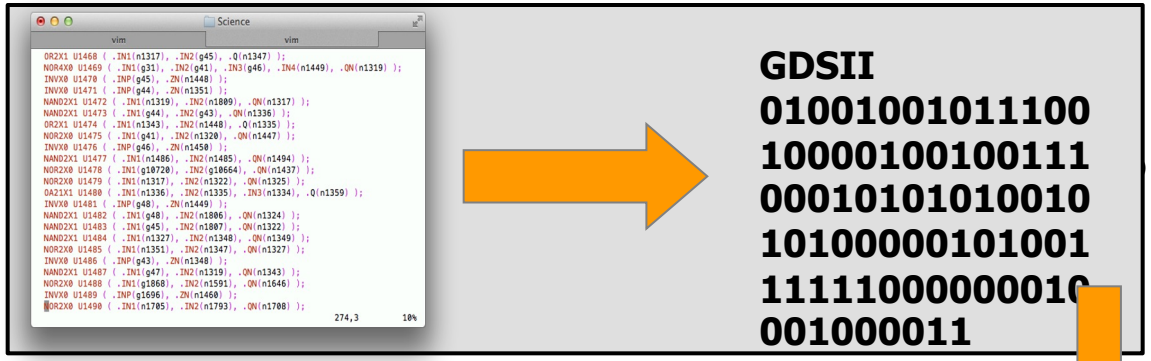
Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

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

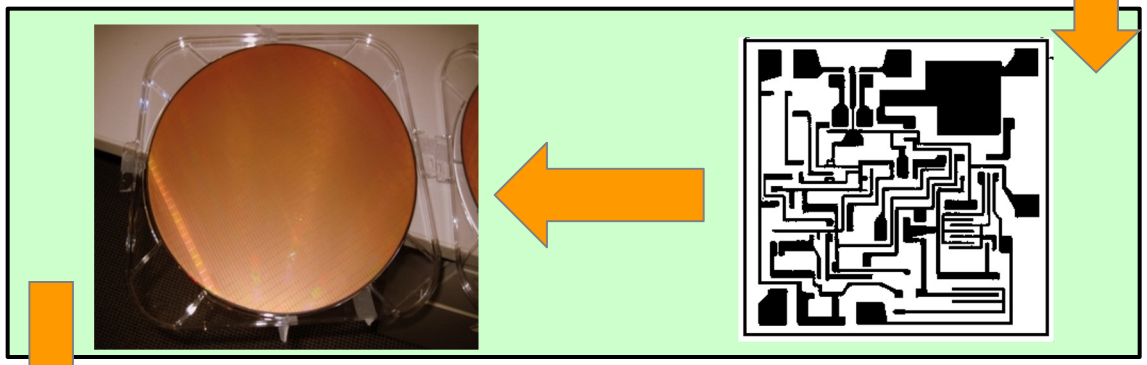
Untrusted System Integrator



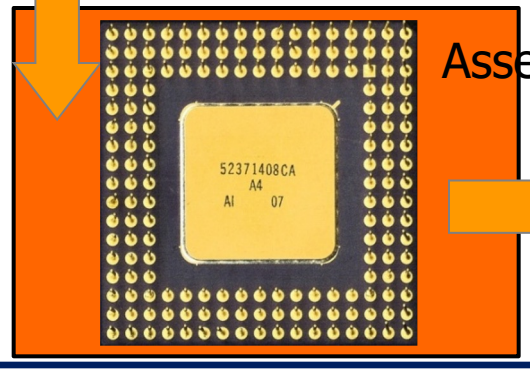
Counterfeiting



Owner



Foundry

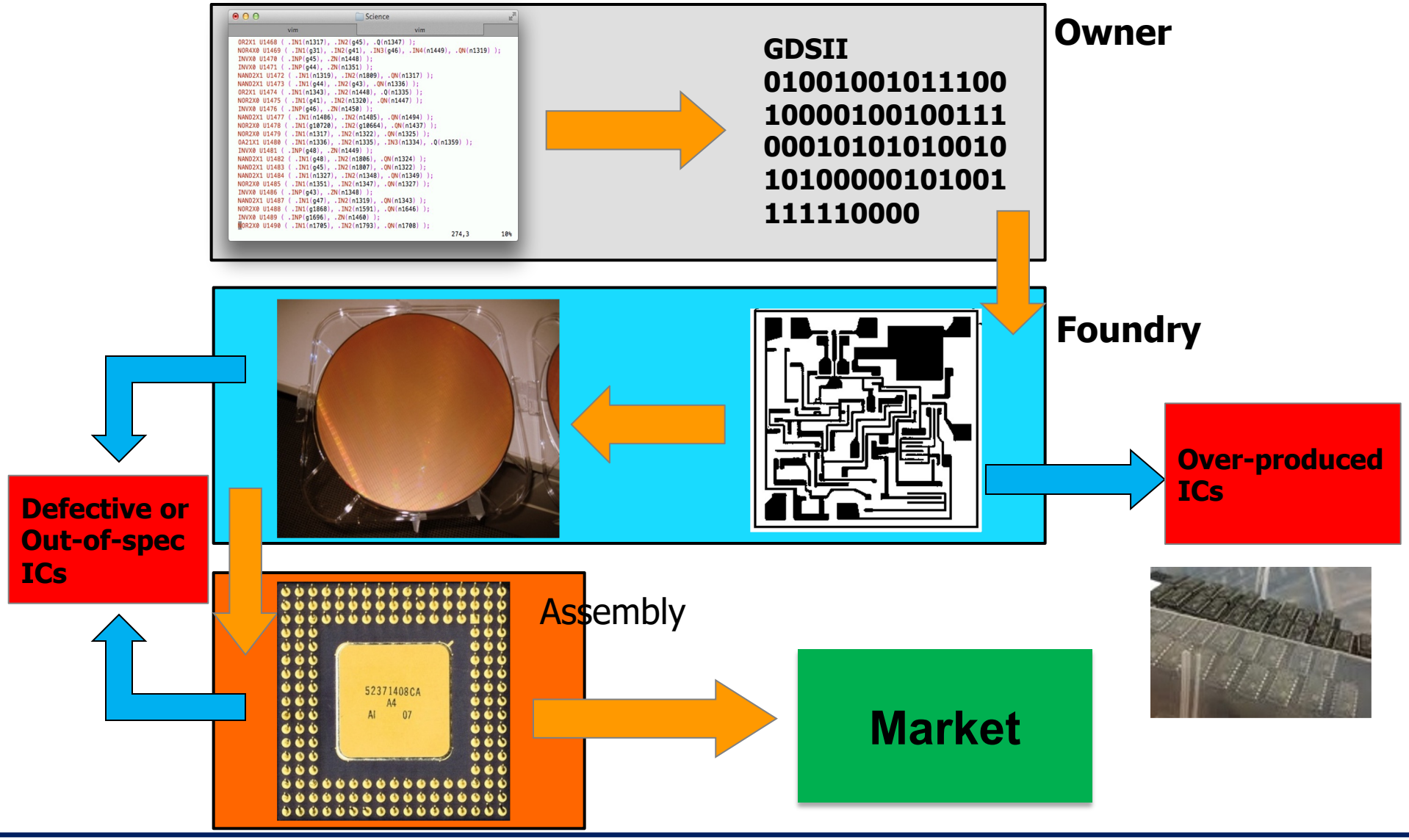


Assembly

Market

Google image

Counterfeiting



Google image

IC Counterfeiting

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

Over production

Off-spec parts

Defective parts

Cloned ICs

Recycled ICs

IC Recycling Process

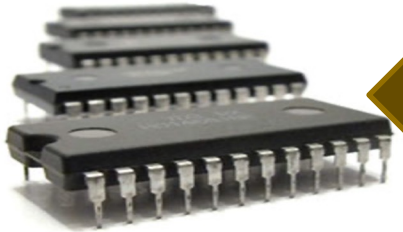
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new



Critical Application

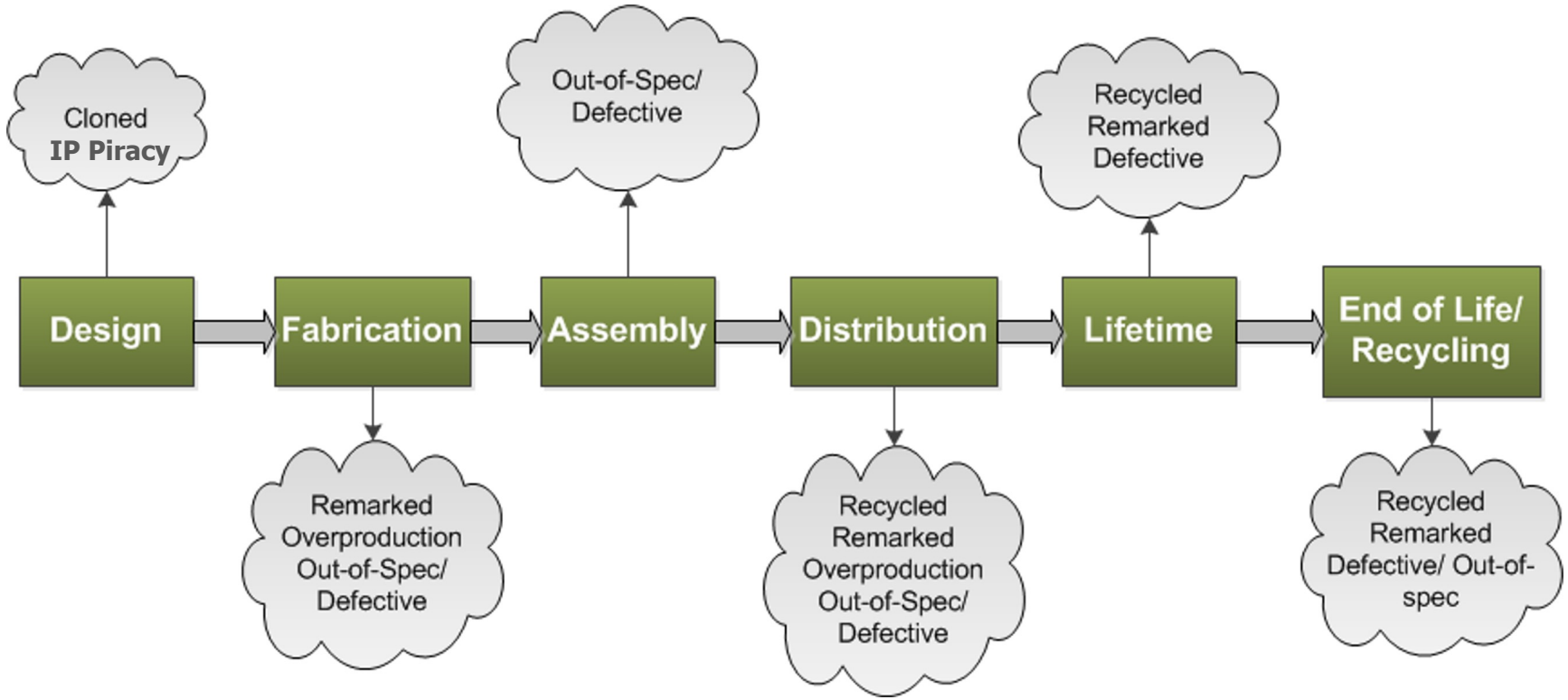
Identical:

Appearance, Function, Specification

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

Source: Images are taken from google

Supply Chain Vulnerabilities



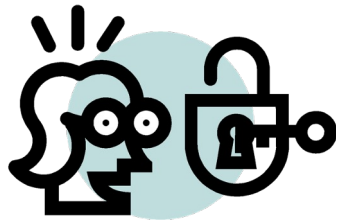
Some Basic Definitions

- **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)
    - the science of locks and keys
  - The keys and locks are mathematical
  - Underlying every security mechanism, there is a "secret"…
  - 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



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 and vulnerabilities
- 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
- Tampering
- Reverse Engineering

Adversaries

- **Individual, group or governments**
  - Pirating the IPs – illegal use of IPs
  - Inserting backdoors, or malicious circuitries
  - 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.

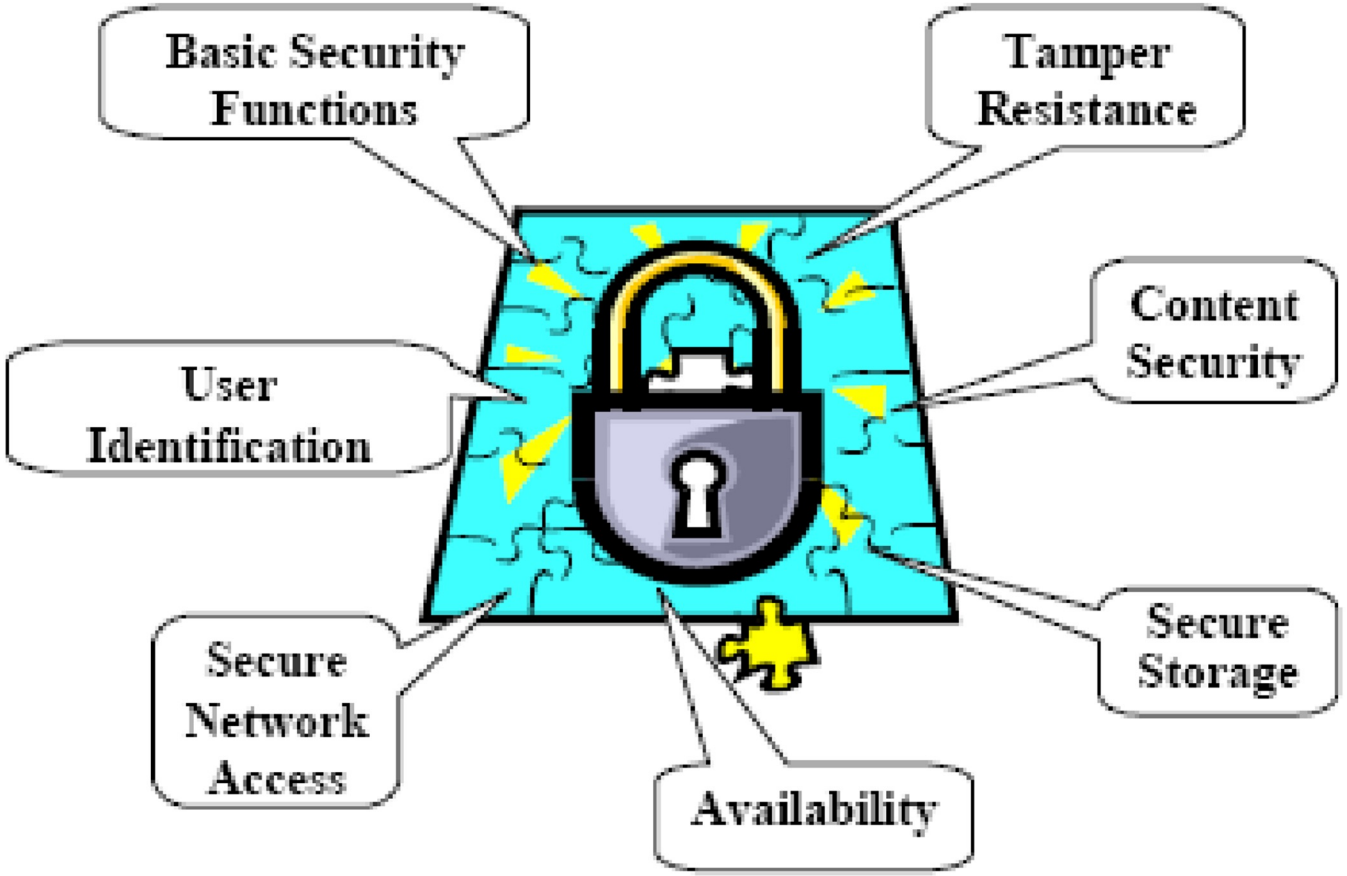
Hardware Controls for Secure Systems

- 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
- More …

Embedded Systems Security/IoTs

- Security processing adds overhead
  - Performance and power
- Security is challenging in embedded systems/IoTs
  - 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 in the IoT Era



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

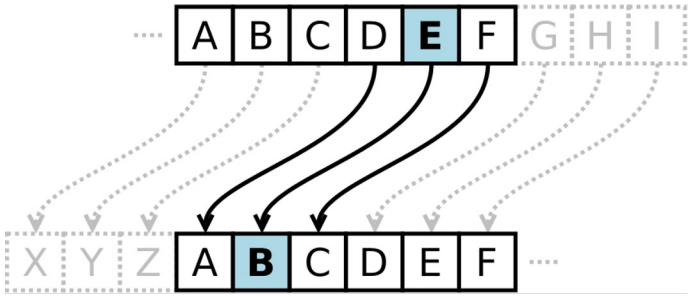
- **Underlying most security mechanisms or protocols is the notion of a "secret"**
  - Lock and keys
  - Passwords
  - Hidden signs and procedures
  - Physically hidden

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



Plaintext: THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Ciphertext: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

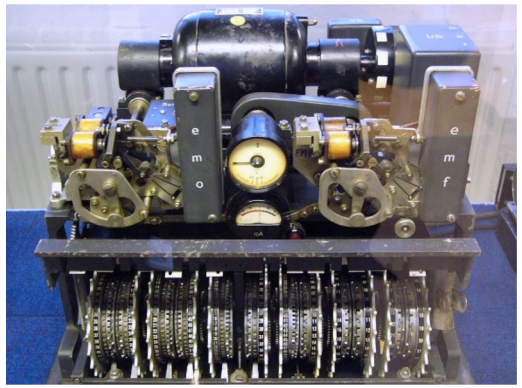
- Cryptoquote: simple substitution cipher, permutations of 26 letters
  - Using the dictionary and the frequencies, this is also easy to break

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 (Lorenz cipher system)
- 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: $c=p \oplus ks$
- How was this code cracked by British cryptographers at Bletchley Park in Jan 1942?
- A lucky coincidence!



German rotor stream cipher machines used by the German Army during World War II

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