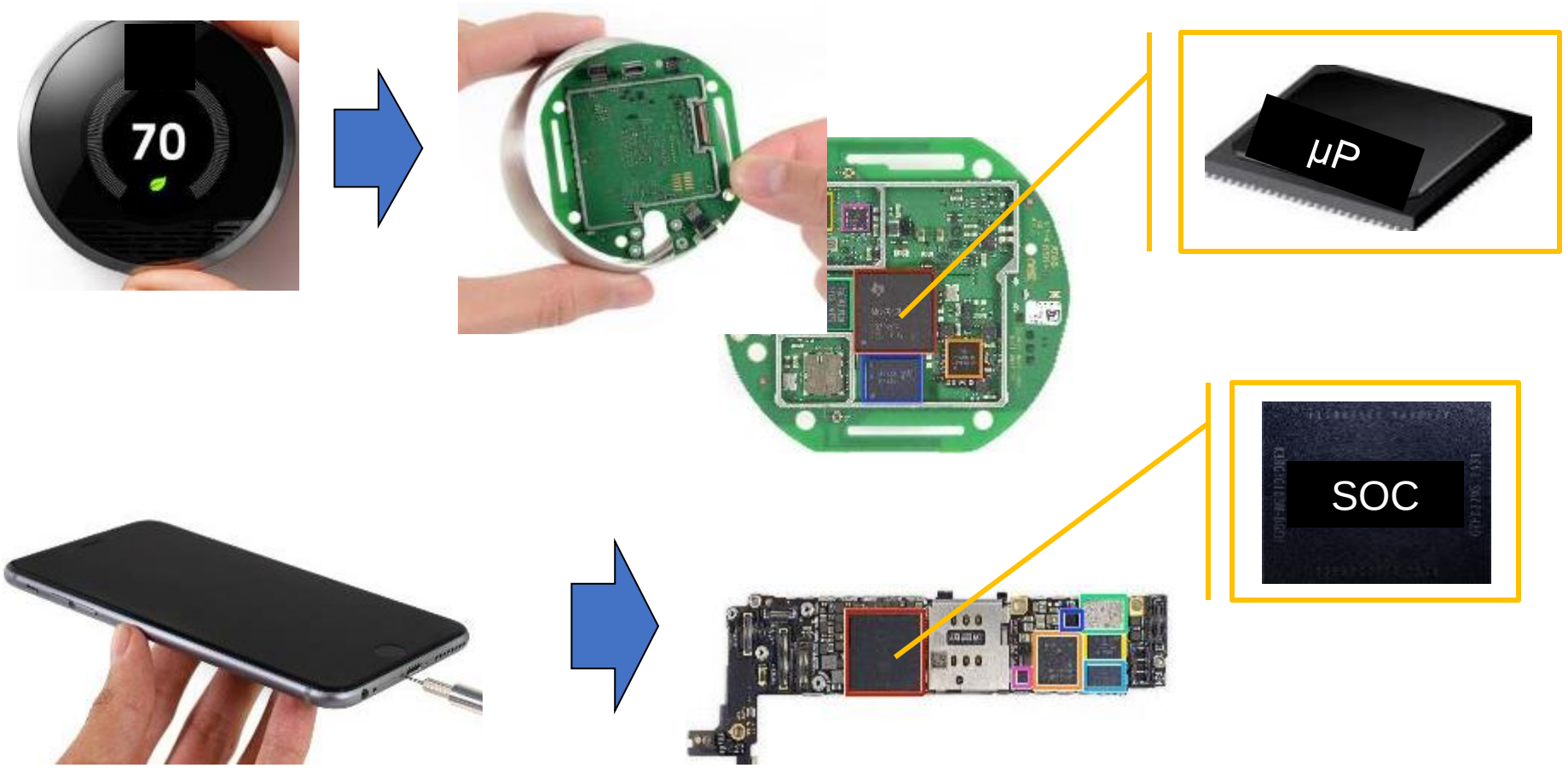
Hardware Security

Cybersecurity experts have traditionally assumed that the hardware underlying information systems is secure and trusted. However such assumption is no longer true.

What is Hardware?



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

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.

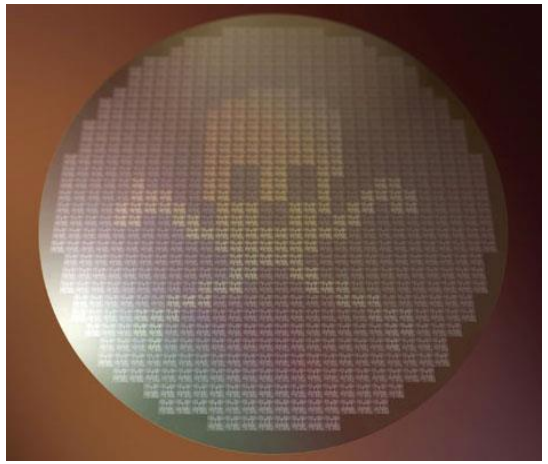
Example Attack

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

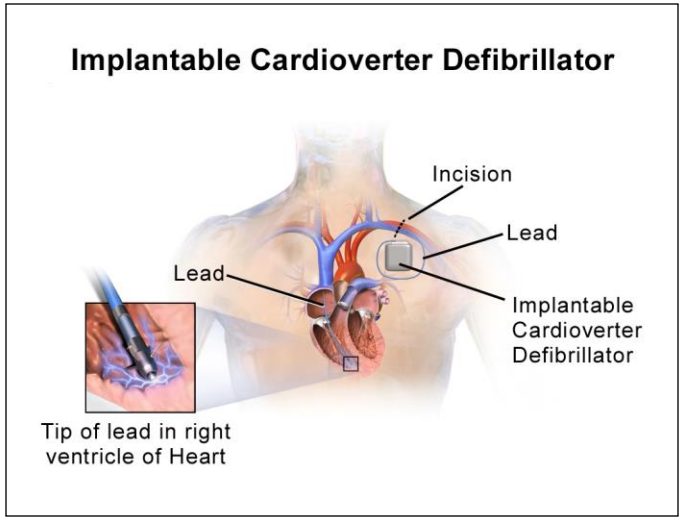
Example Attack

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



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!

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!

Example Attack

Physical Attacks on Chip IDs

- Extracting secret keys

Side-Channel Attacks

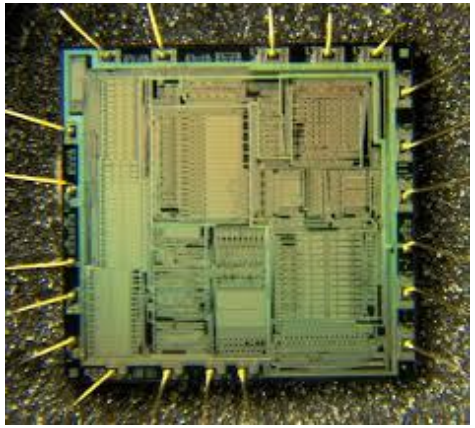
- Power Analysis, Timing Analysis, EM Analysis

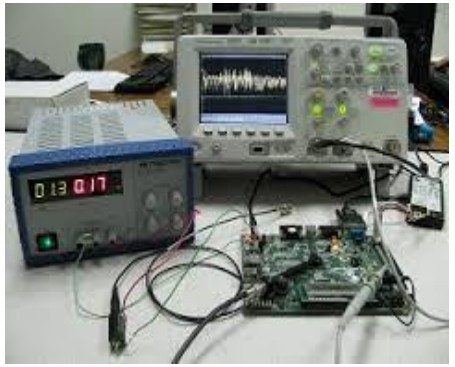
Tampering with Electronic Devices

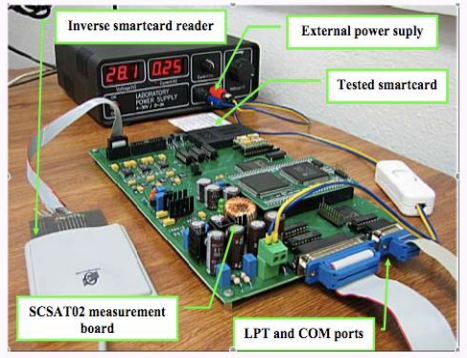
- Captured Drone by Iran

Counterfeit Integrated Circuits

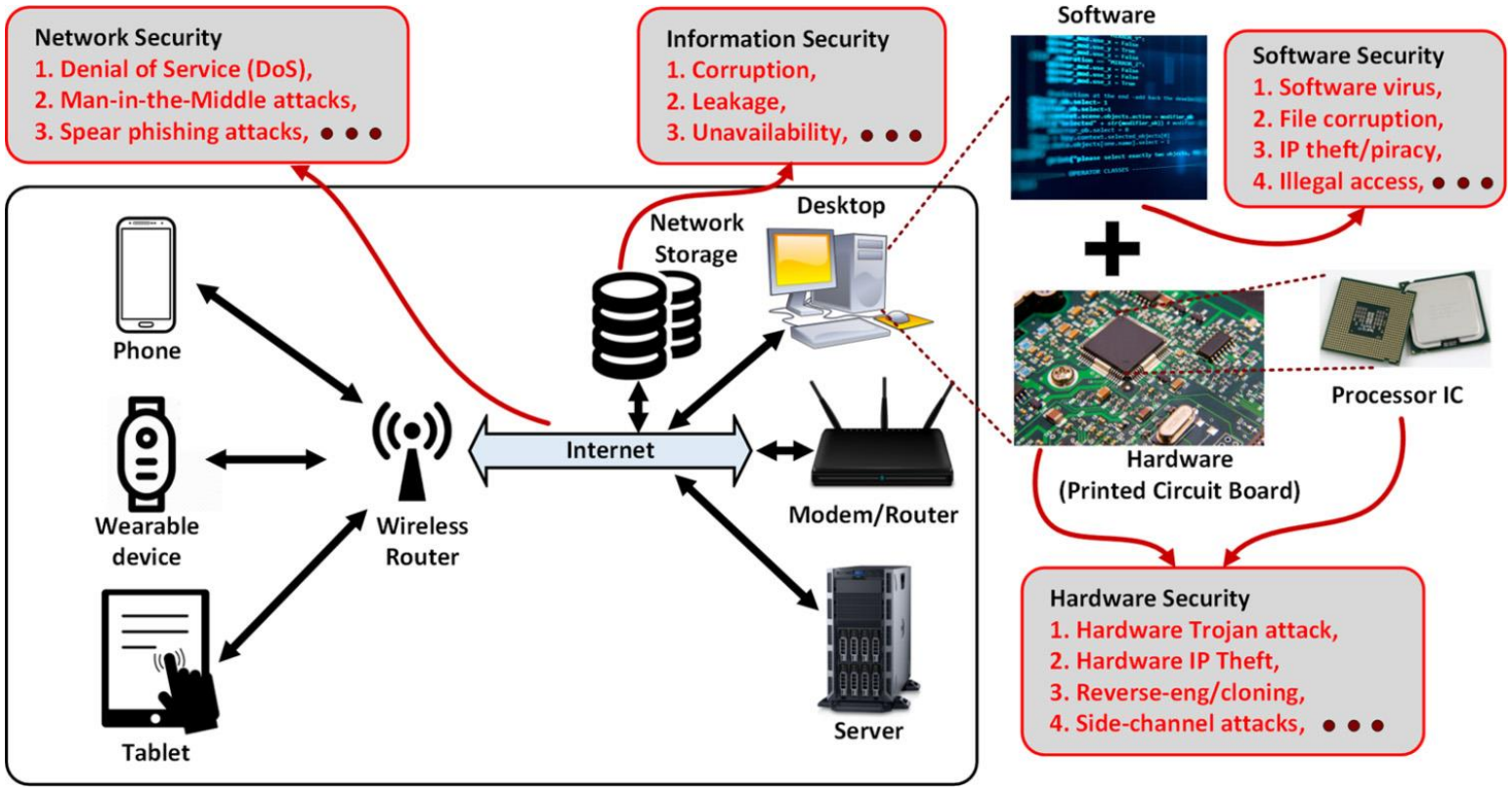
- Multi-billion dollar business



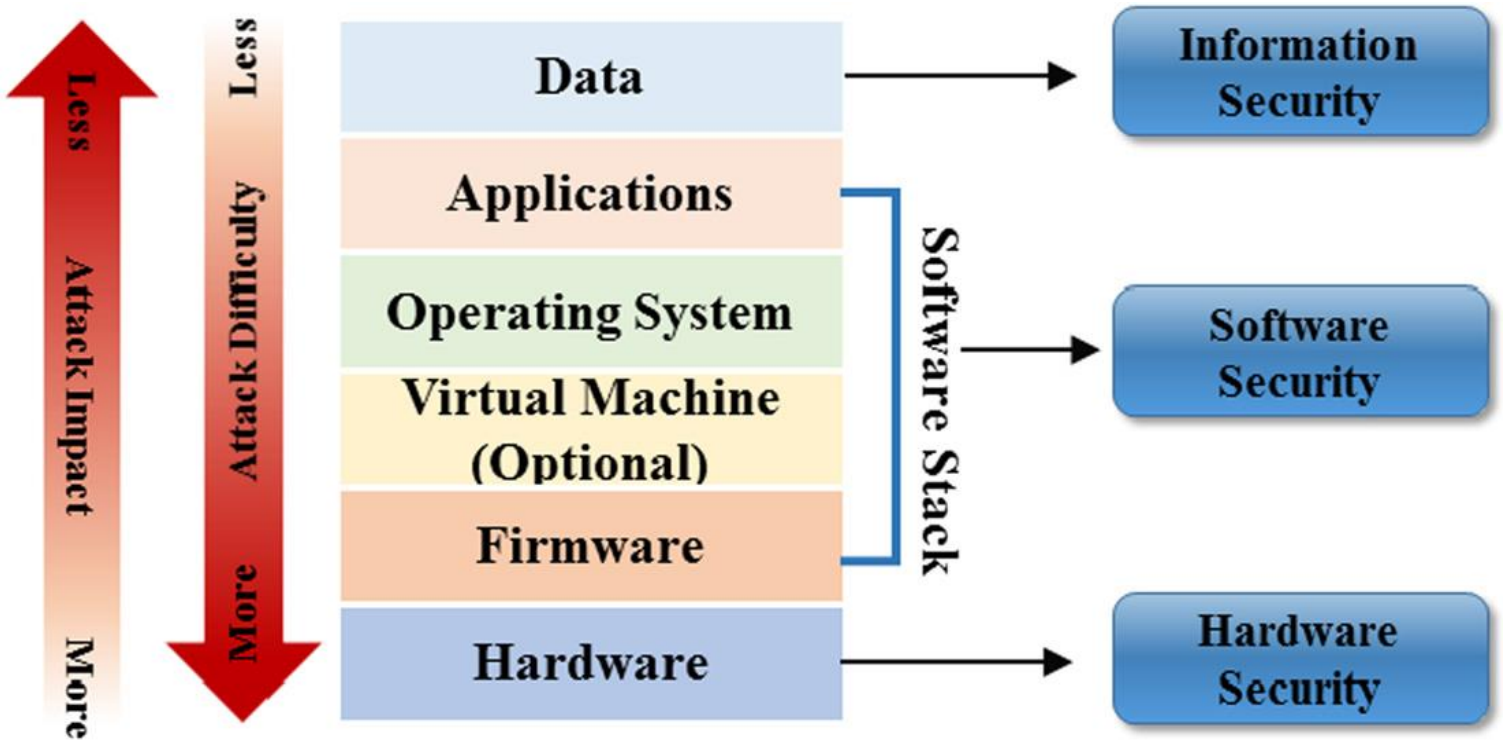




The landscape of Security in Modern Computing Systems

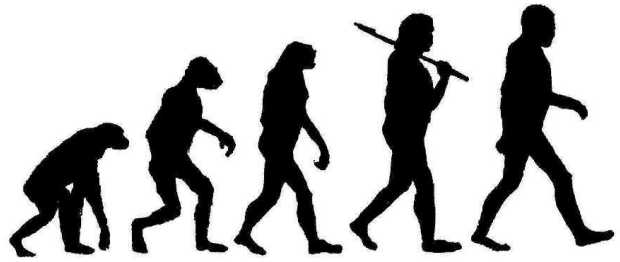


Attack impact and difficulty at different layers of a computing system

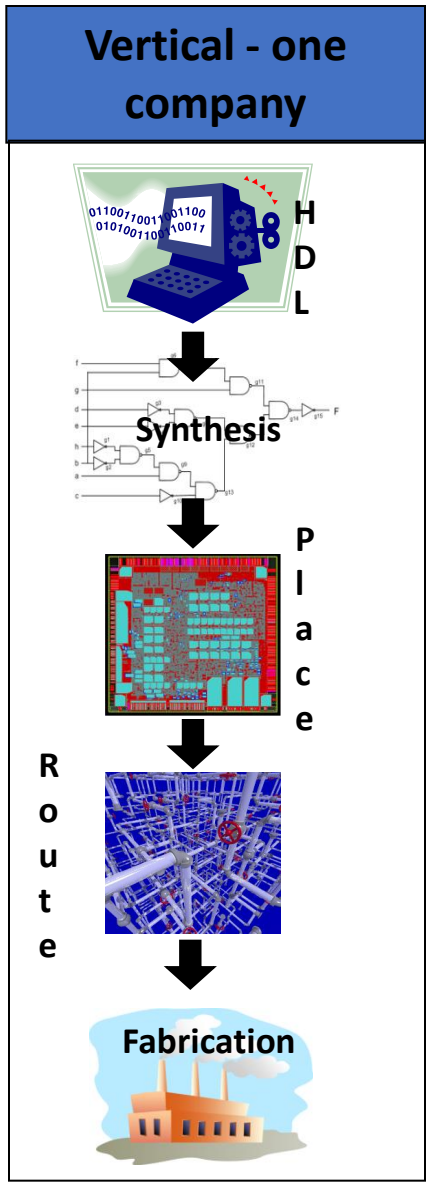


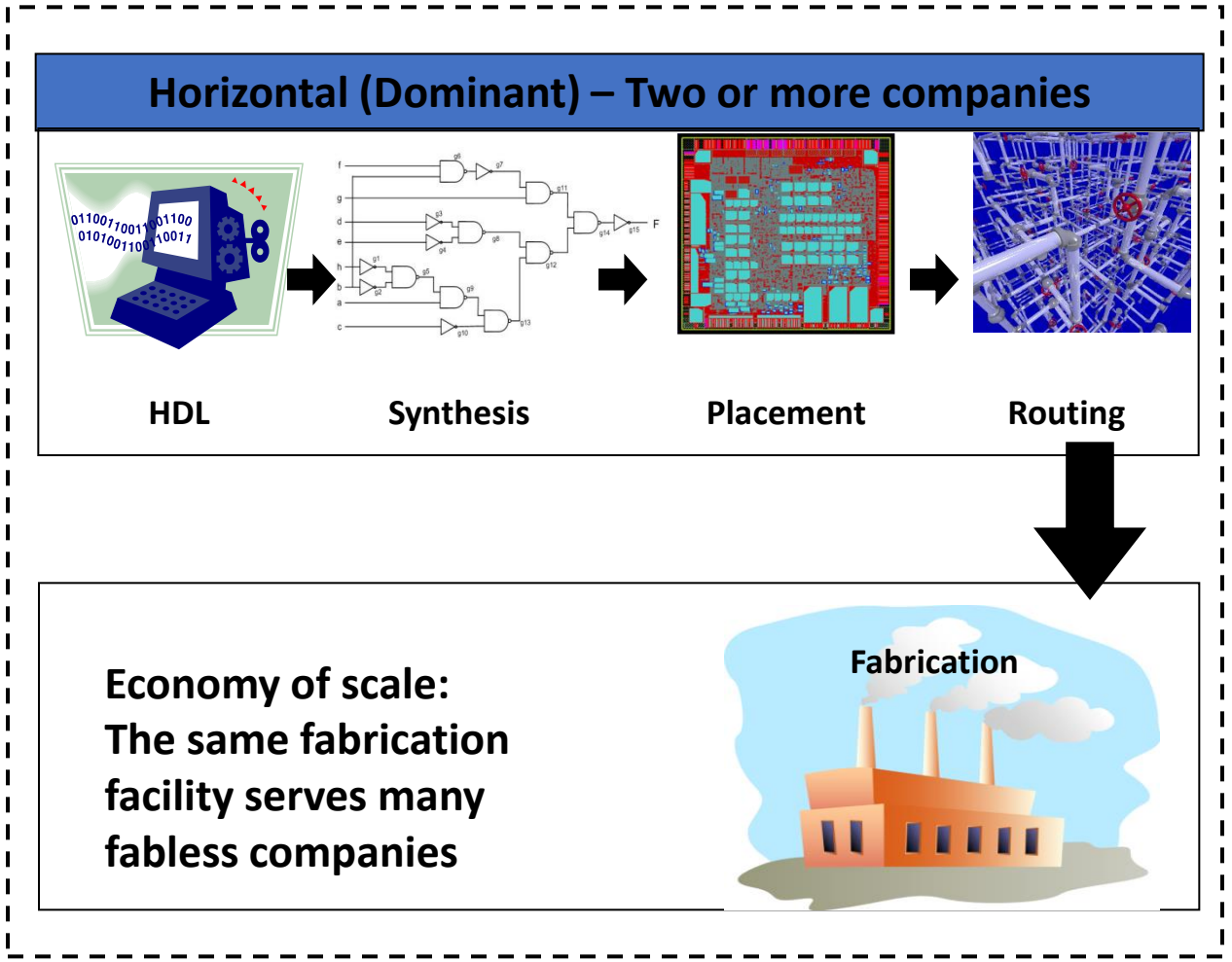
Evolution of Hardware Security and Trust

- **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…



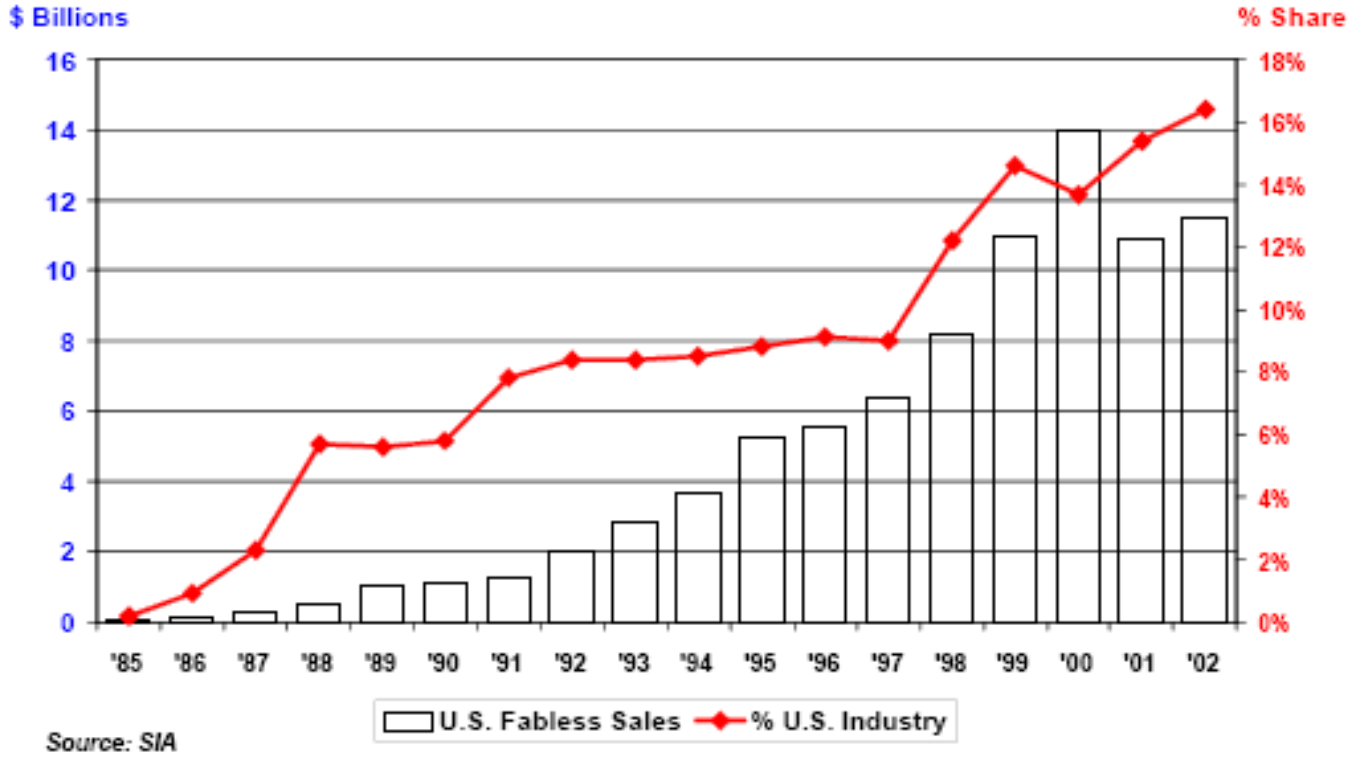
Shift in the Industry's Business Model





Microelectronic Industry Business Model

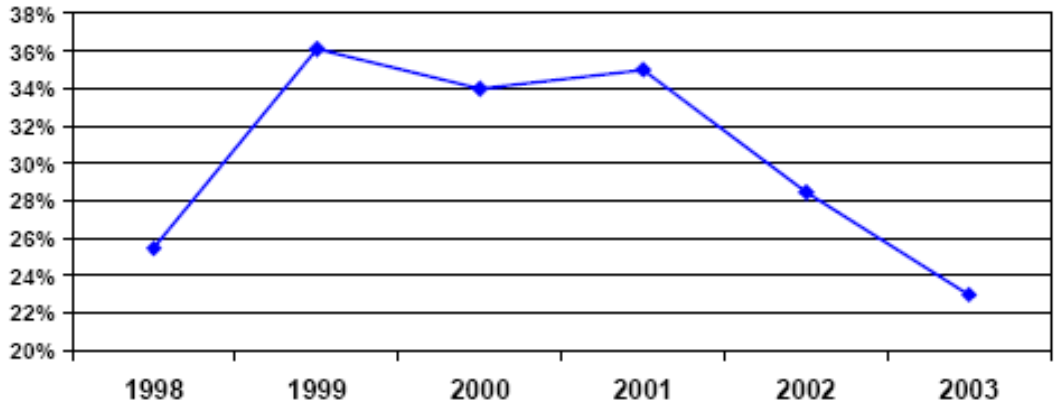
The fabless/foundry business model has grown to 16% of the U.S. chip industry. The trend is strongest in the leading process technology portion of the industry



Source: SIA

Leading-Edge Technology

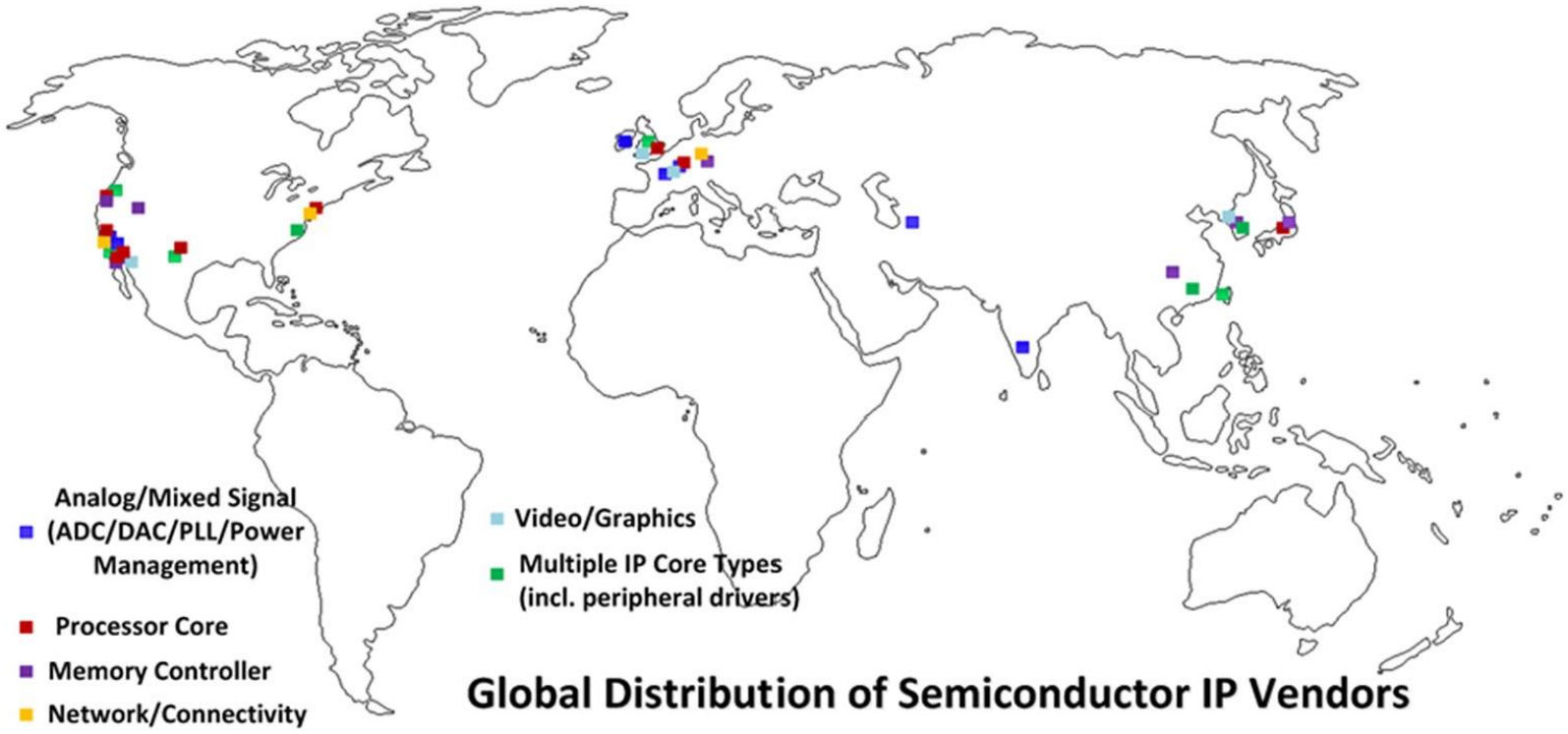
U.S. industry's share of capital expenditures falling and in leading edge semiconductor manufacturing capacity.



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

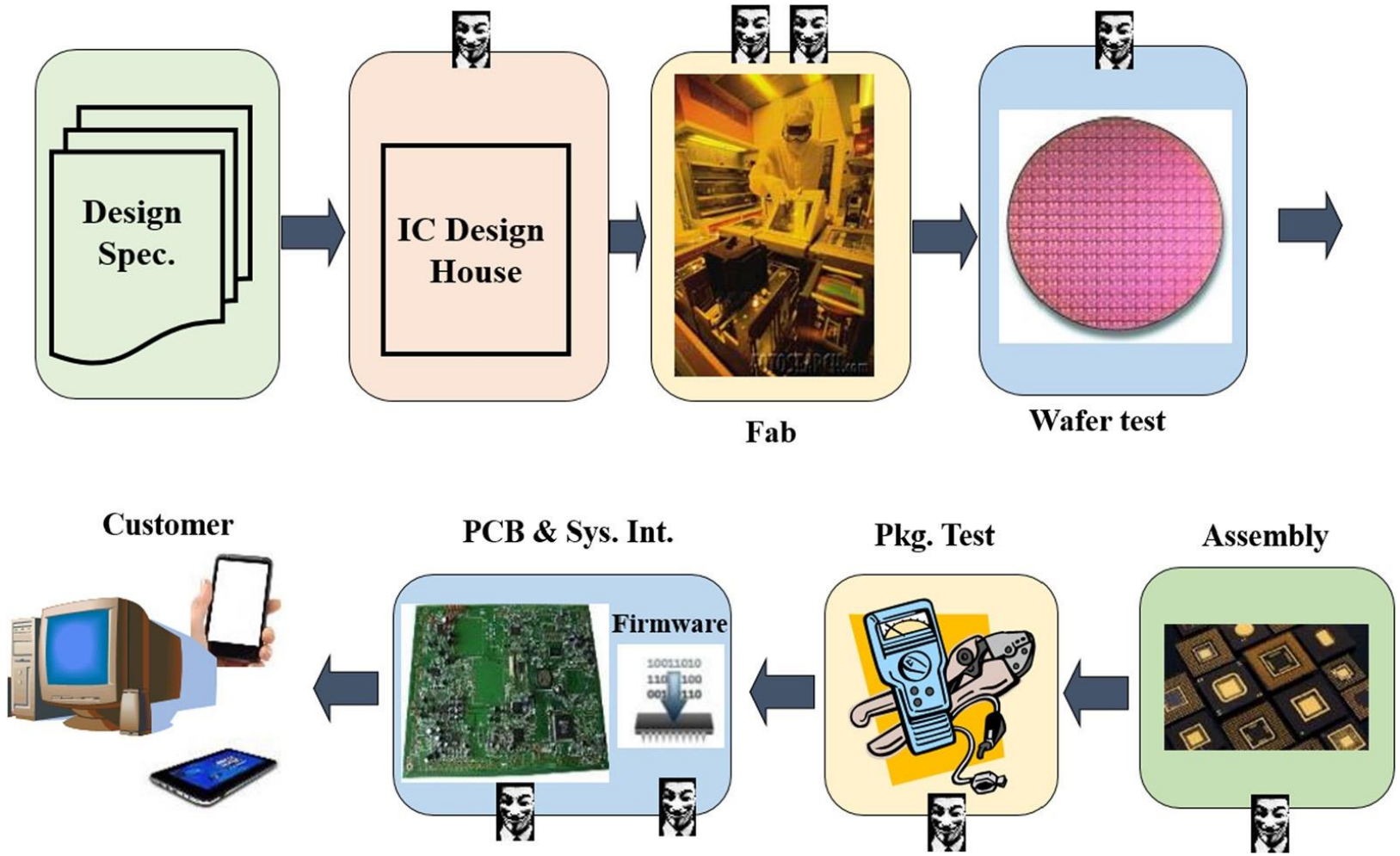
Source: SICAS/SIA

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

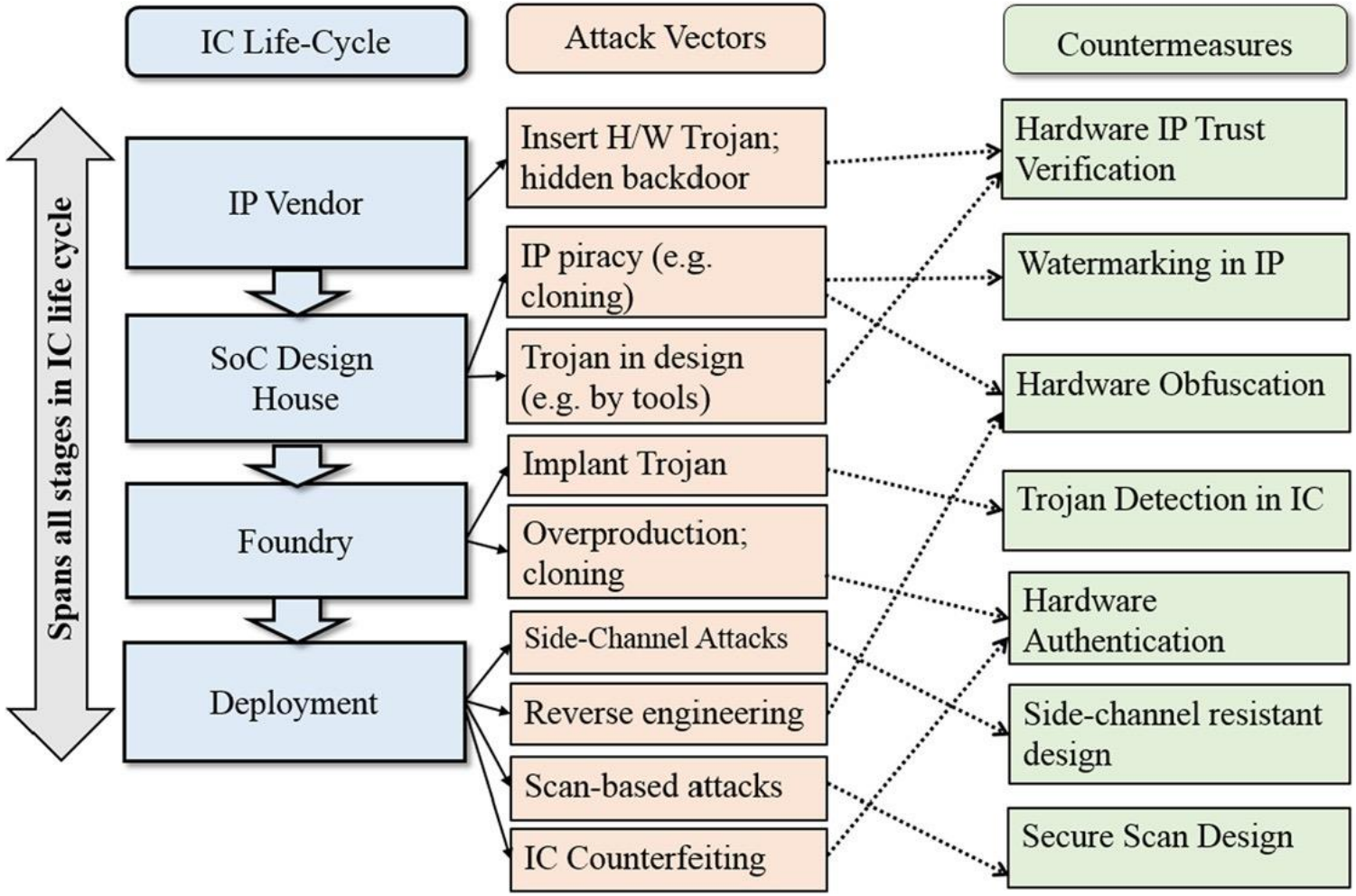


Long and globally distributed supply chain of hardware IPs makes SoC design increasingly vulnerable to diverse trust/integrity issues.

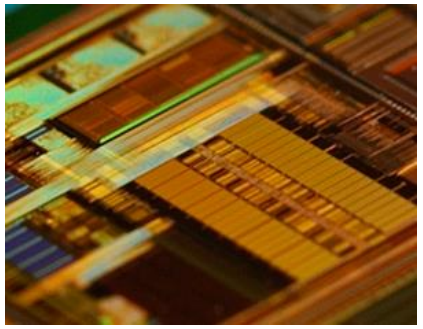
Major steps in the electronic hardware design and test flow

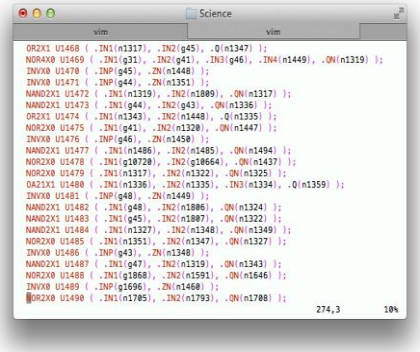


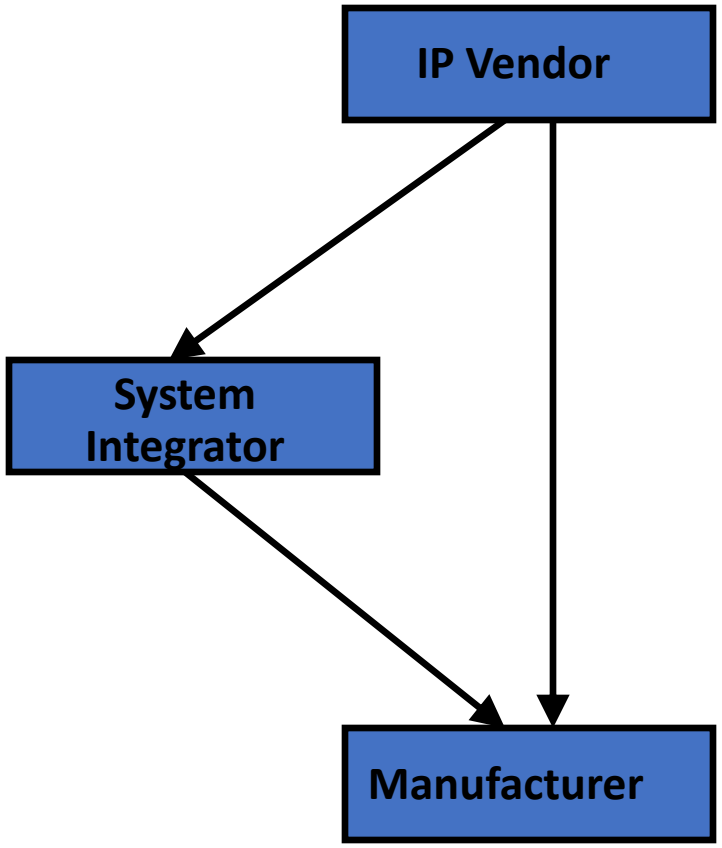
Attack vectors and countermeasures



HW Threats

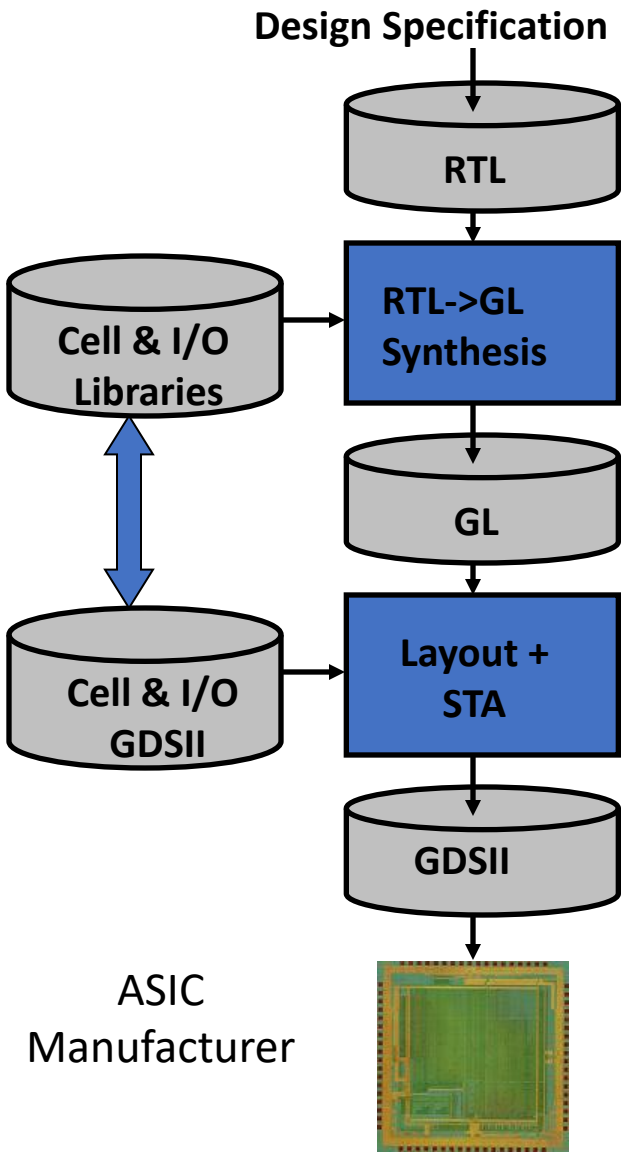






Any of these steps can be untrusted

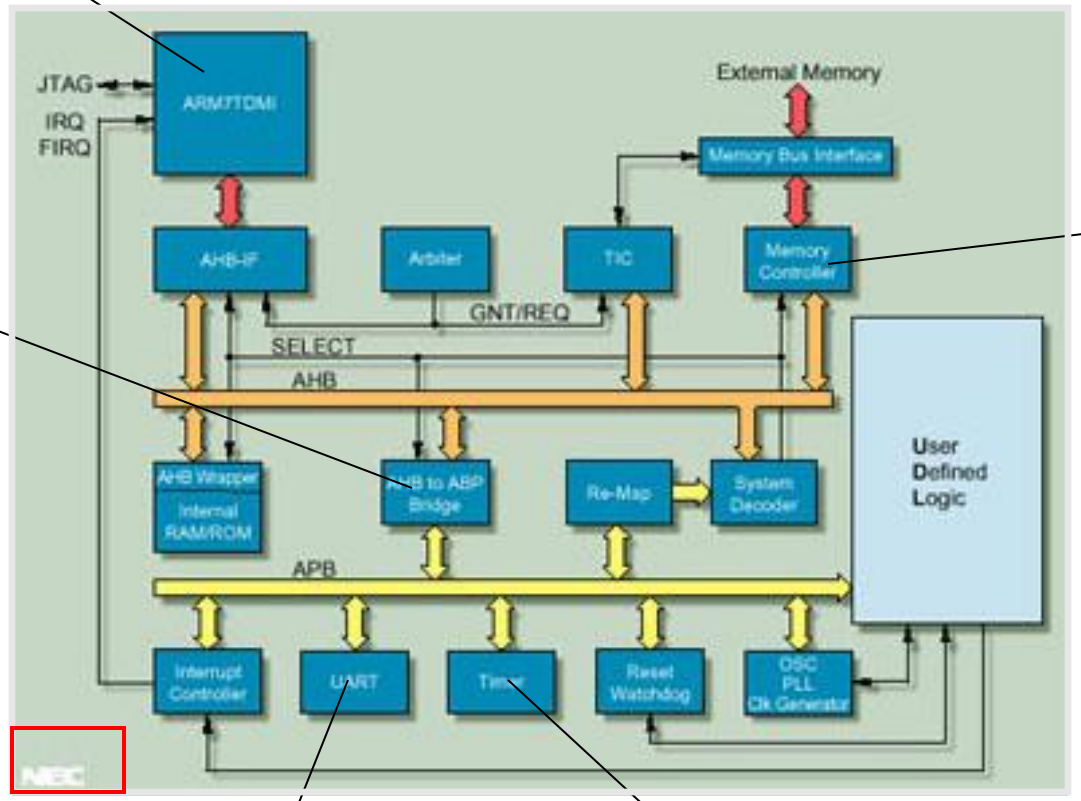
Design Process – Old Way



Issues with Third-Party IP Design

Company X

System-on-Chip (SoC)



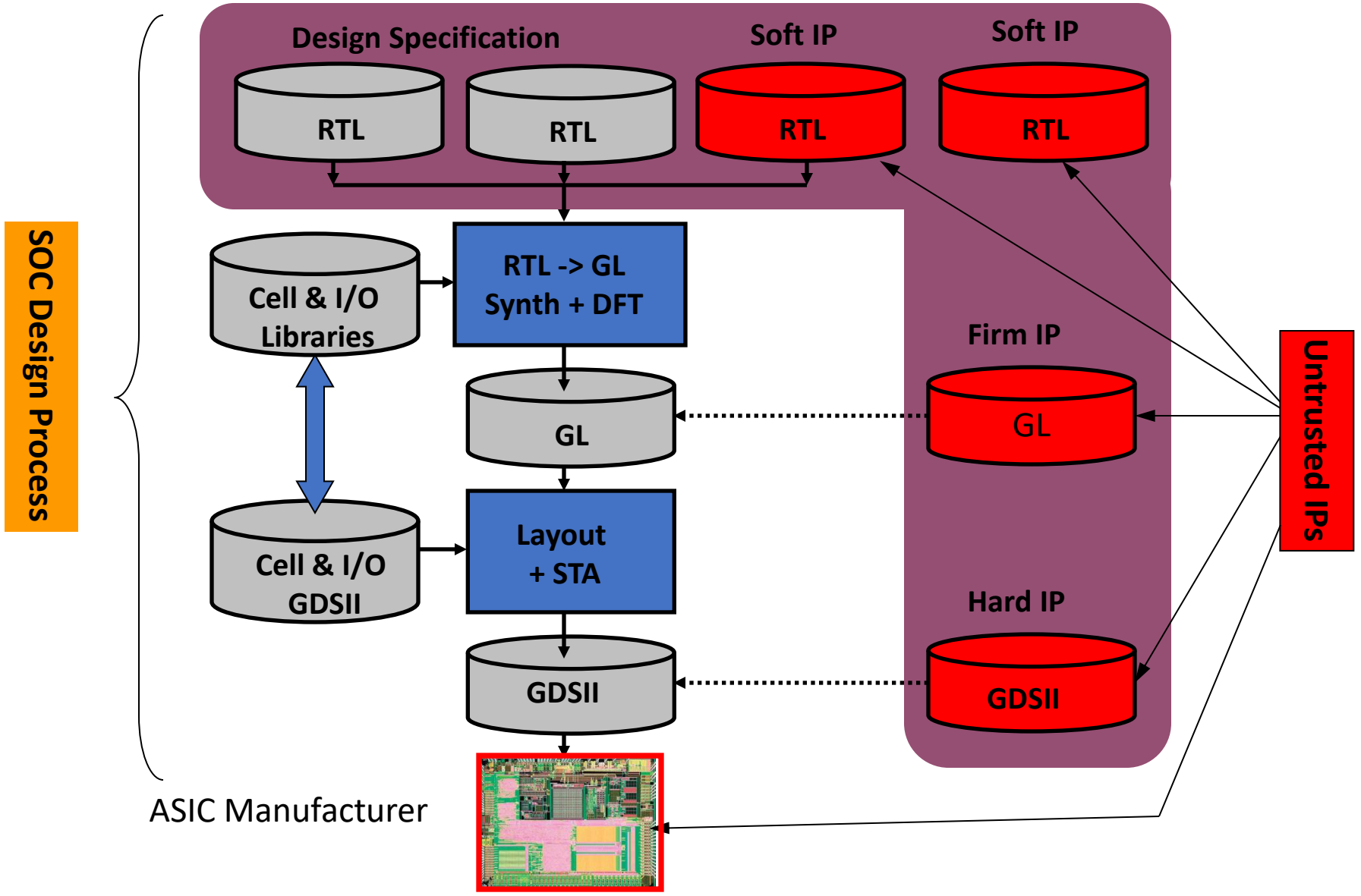
Company Y

Company Z

Company V

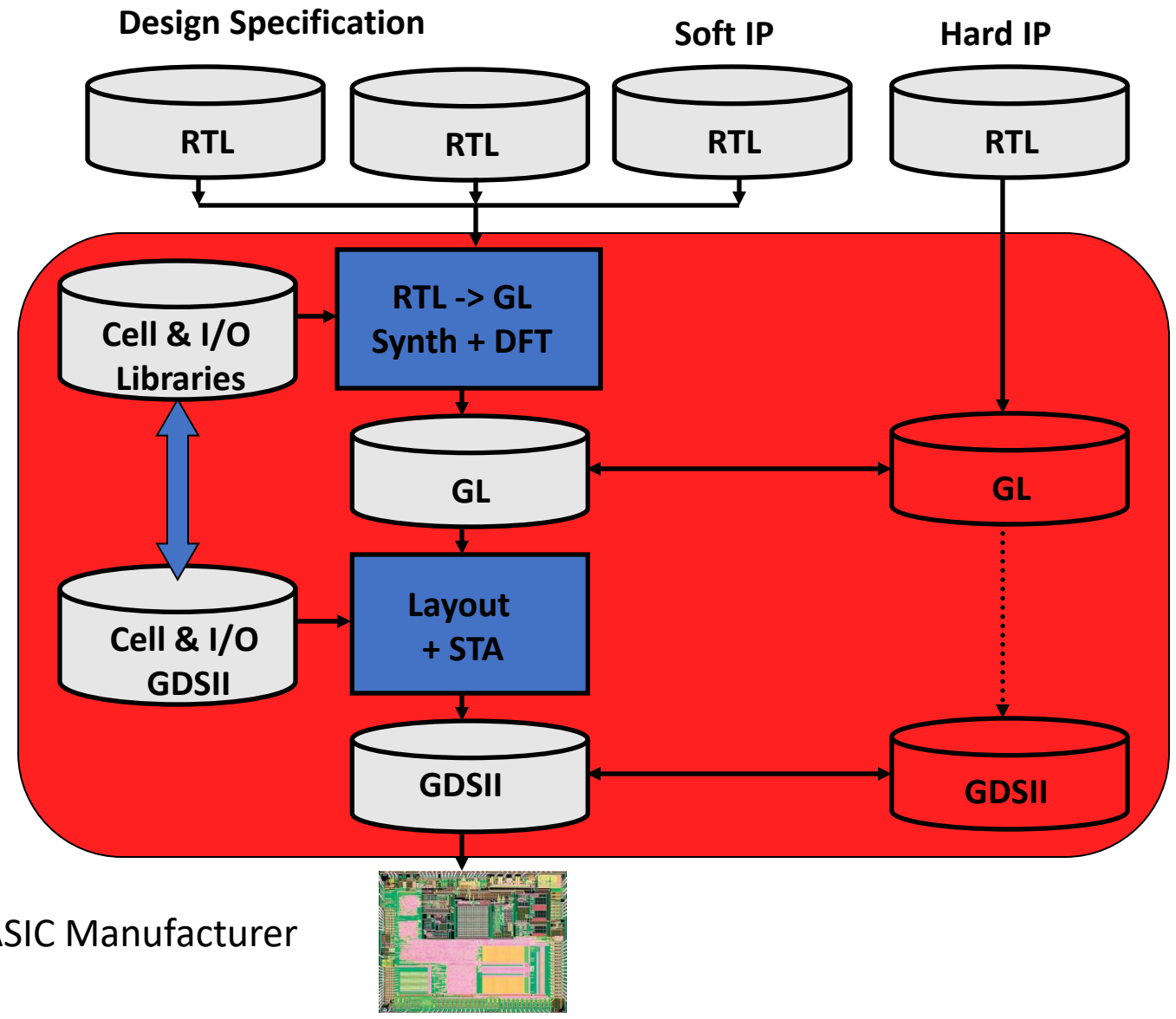
Company W

Design Process – New Way



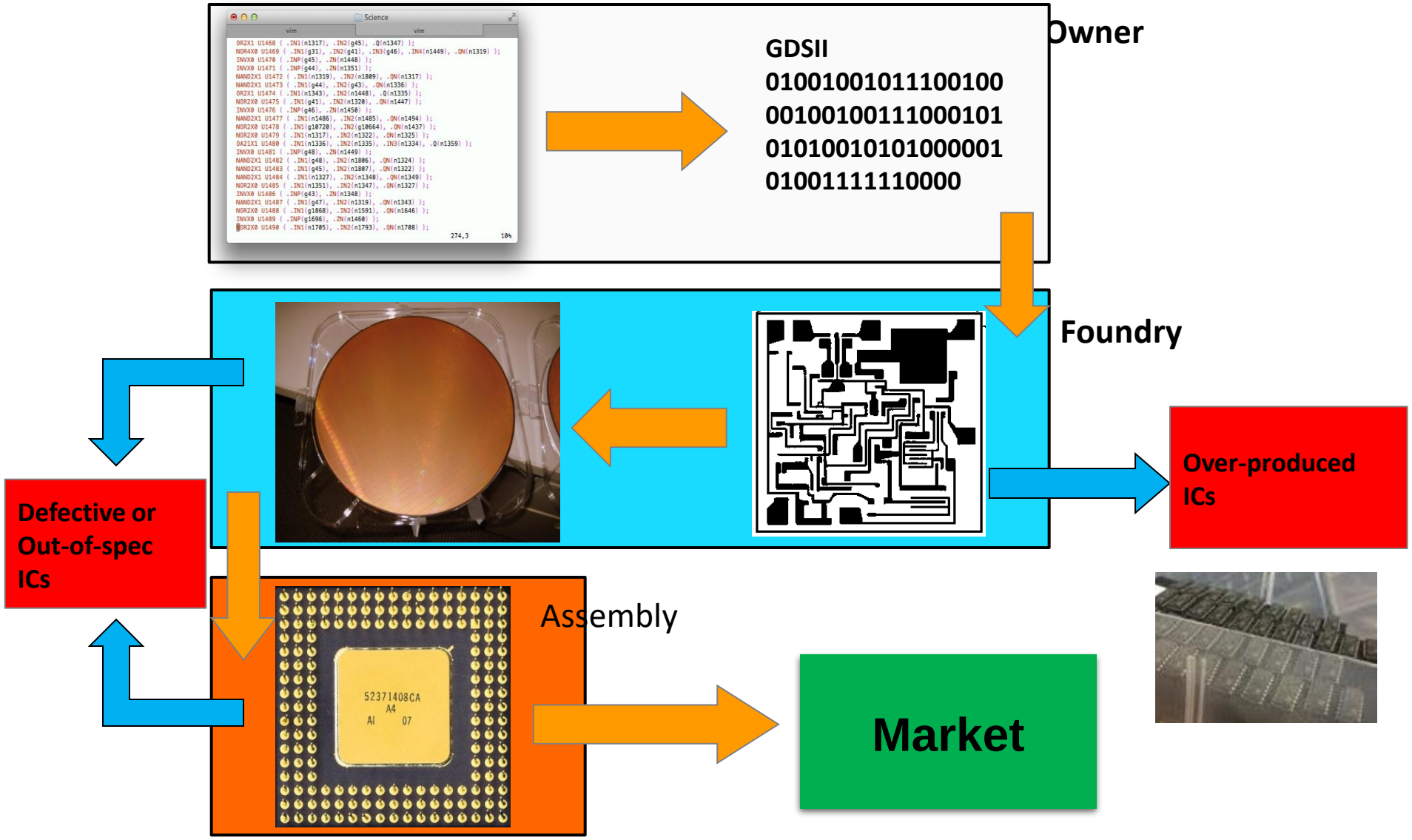
Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

Untrusted System Integrator



ASIC Manufacturer

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

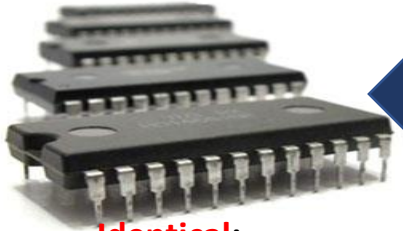
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new



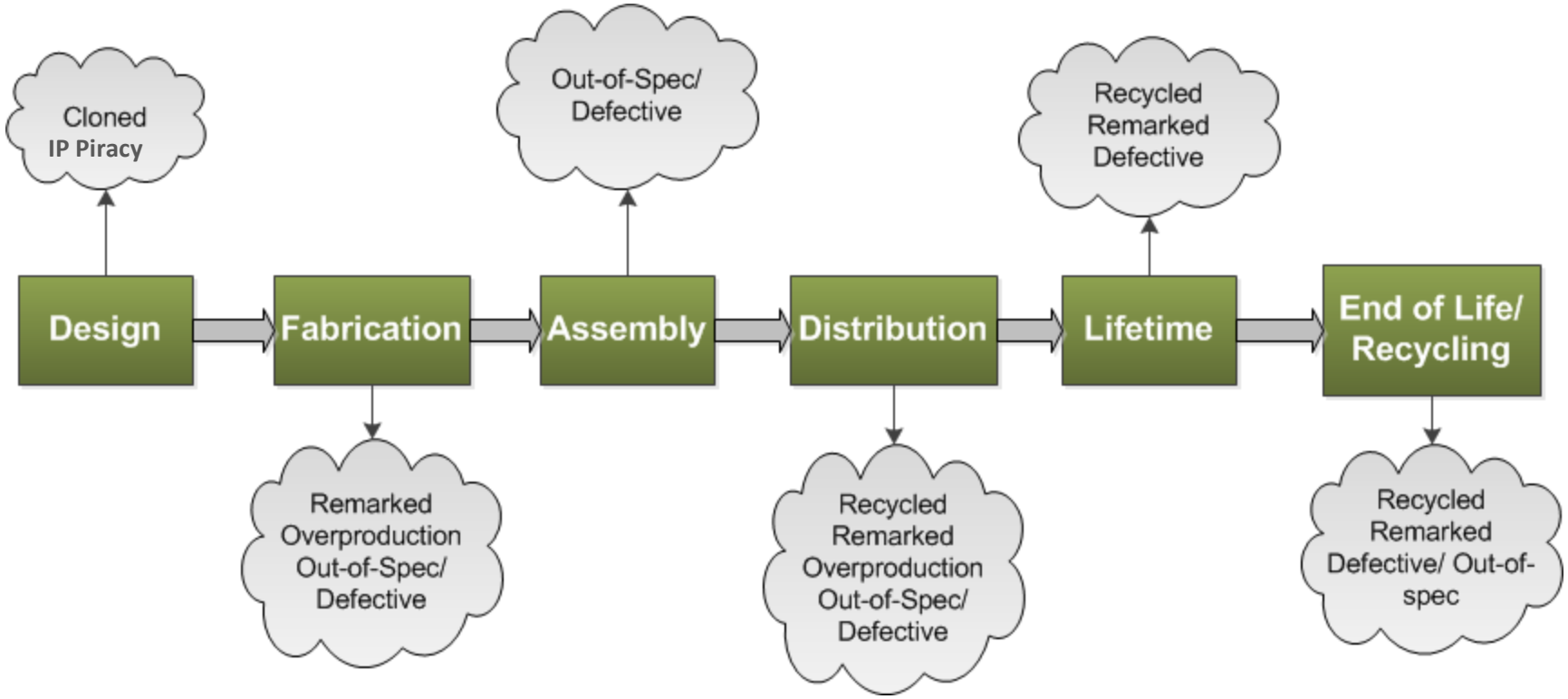
Identical:
Appearance, Function, Specification

Critical Application

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

Source: Images are taken from google

Supply Chain Vulnerabilities



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.

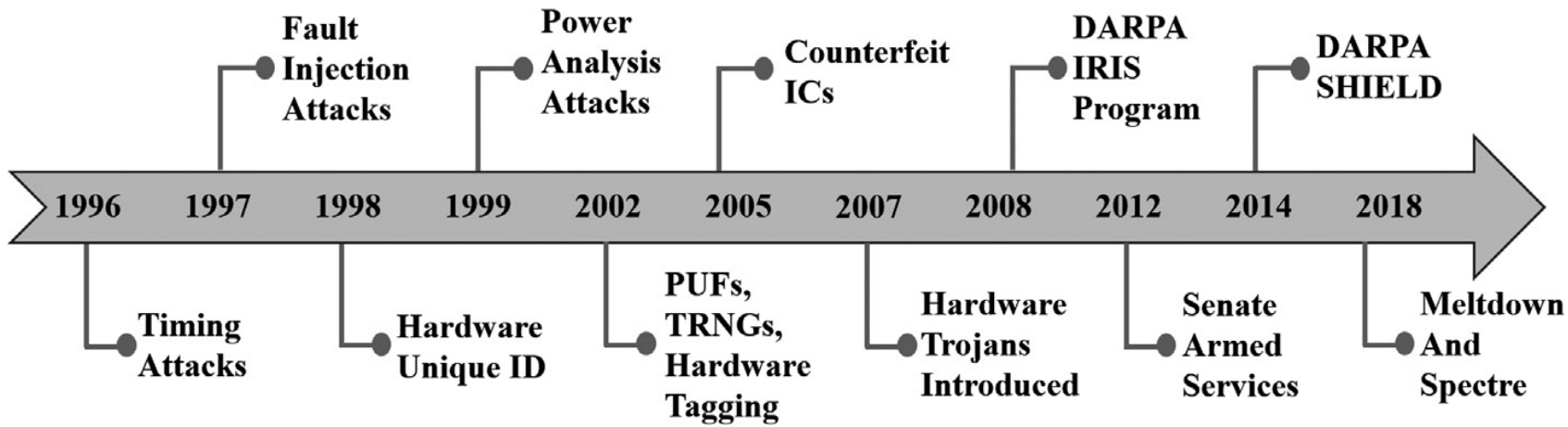

1996
1997
1998
1999
2002
2005
2007
2008
2012
2014
2018
Timing Attacks
Fault Injection Attacks
Hardware Unique ID
Power Analysis Attacks
PUFs, TRNGs, Hardware Tagging
Counterfeit ICs
Hardware Trojans Introduced
DARPA IRIS Program
Senate Armed Services
DARPA SHIELD
Meltdown And Spectre

Table 1.1 Bird's-eye view of the hardware attacks & countermeasures

Attacks					
Type of Attack	**What it is**	**Adversary**	**Goal**	**Life-cycle stages**	**Chapter #**
Hardware Trojan Attacks	Malicious design modification (in chip or PCB)	Untrusted foundry, untrusted IP Vendor, untrusted CAD tool, untrusted design facilities	• Cause malfunction • Degrade reliability • Leak secret info	• Design • Fabrication	Chapter 5
IP Piracy	Piracy of the IP by unauthorized entity	Untrusted SoC Designer, untrusted foundry	• Produce unauthorized copy of the design • Use an IP outside authorized use cases	• Design • Fabrication	Chapter 7
Physical Attacks	Causing physical change to hardware or modifying operating condition to produce various malicious impacts	End user, bad actor with physical access	• Impact functional behavior • Leak information • Cause denial of service	• In field	Chapter 11
Mod-chip Attack	Alteration of PCB to bypass restrictions imposed by system designer	End user	• Bypass security rules imposed through PCB	• In field	Chapter 11
Side-Channel Attacks	Observing parametric behaviors (i.e., power, timing, EM) to leak secret information	End user, bad actor with physical access	• Leak secret information being processed inside the hardware	• In field	Chapter 8
Scan-based Attacks	Leveraging DFT circuits to facilitate side-channel attack	End user, bad actor with physical access	• Leak secret information being processed inside the hardware	• In field • Test-time	Chapter 9
Microprobing	Using microscopic needles to probe internal wires of a chip	End user, bad actor with physical access	• Leak secret information residing inside the chip	• In field	Chapter 10
Reverse Engineering	Process of extracting the hardware design	Design house, foundry, end user	• Extract design details of the hardware	• Fabrication • In field	Chapter 7

(continued on next page)

Table 1.1 (*continued*)

Countermeasures					
Type of Countermeasure	**What it is**	**Parties involved**	**Goal**	**Life-cycle stages**	**Chapter #**
Trust Verification	Verifying the design for potential vulnerabilities to confidentiality, integrity, and availability	• Verification engineer	• Provide assurance against known threats	• Pre-silicon verification • Post-silicon validation	Chapter 5
Hardware Security Primitives (PUFs, TRNGs)	Providing security features to support supply chain protocols	• IP integrator • Value added reseller (for enrollment)	• Authentication • Key generation	• Throughout IC supply chain	Chapter 12
Hardware Obfuscation	Obfuscating the original design to prevent piracy and reverse engineering	• Design house • IP integrator	• Prevent piracy • Reverse engineering • Prevent Trojan insertion	• Design-time	Chapter 14
Masking & Hiding	Design solutions to protect against side-channel attacks	• Design house	To prevent side-channel attacks by reducing leakage or adding noise	• Design-time	Chapter 8
Security Architecture	Enable design-for-security solution to prevent potential and emerging security vulnerabilities	• Design house • IP integrator	Address confidentiality, integrity, and availability issues with design-time solution	• Design-time	Chapter 13
Security Validation	Assessment of security requirements	• Verification and validation engineer	Ensure data integrity, authentication, privacy requirements, access control policies	• Pre-silicon verification • Post-silicon validation	Chapter 16