Introduction to IC Hardware Security & Trust

Goals

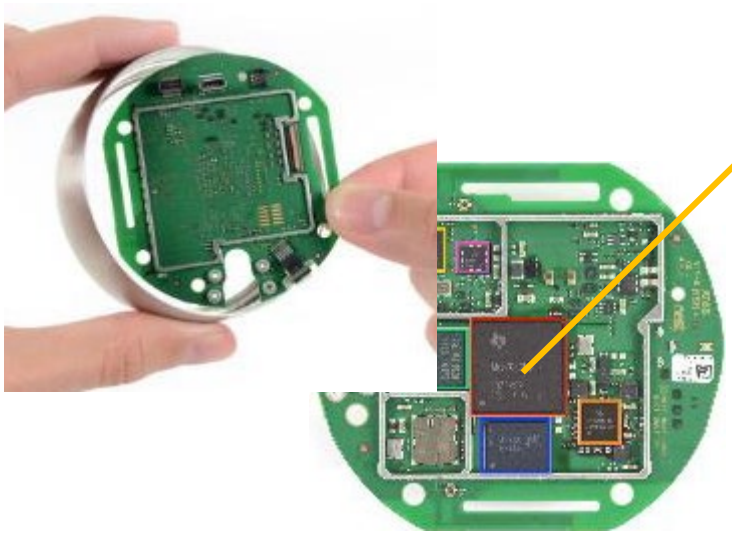
- Learning the state-of-the-art security primitives and methods as well as emerging technologies and security trends
- Integration of security as a design metric, not as an afterthought for the system
- Protection of the design intellectual property against piracy and tampering
- Better understanding of attacks and providing countermeasures against them
- Better understanding of vulnerabilities in design and fabrication processes
- Better understanding of electronic component supply chain vulnerabilities

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)

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
  - 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 (1)

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 through 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.

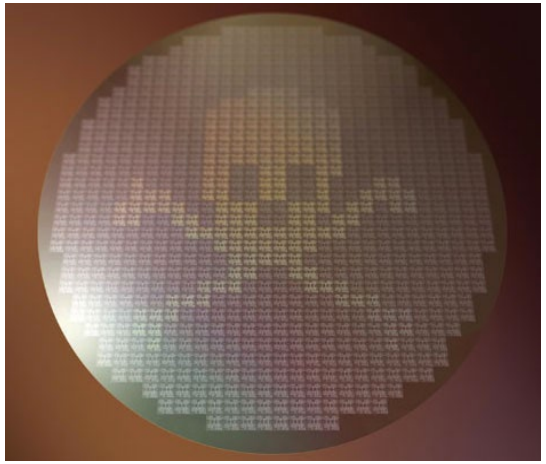
Example Attack (2)

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 (3)

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 because of electricity theft

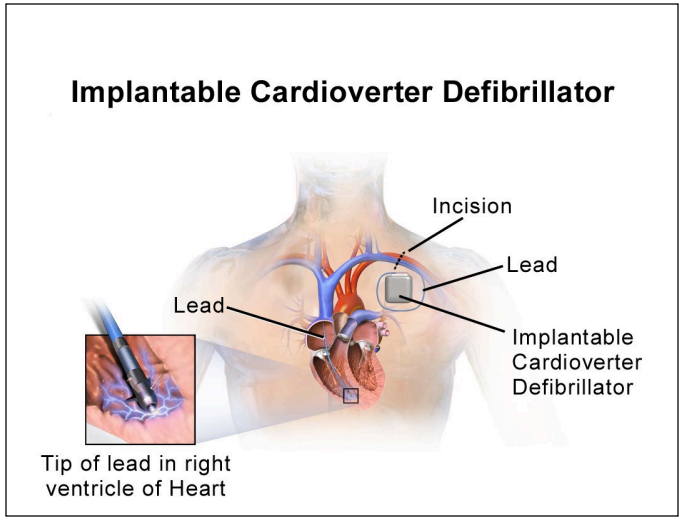
Example Attack (4)

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 (5)

Physical Attacks on Chip IDs

- Extracting secret keys

Side-Channel Attacks

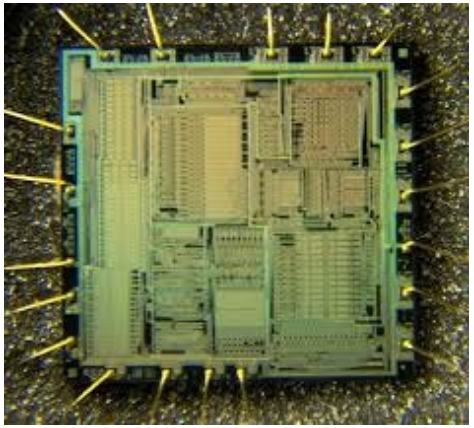
- Power Analysis, Timing Analysis, EM Analysis

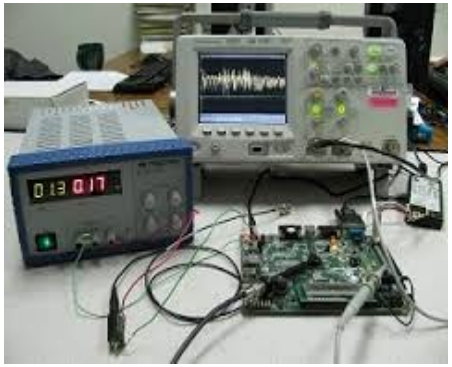
Tampering with Electronic Devices

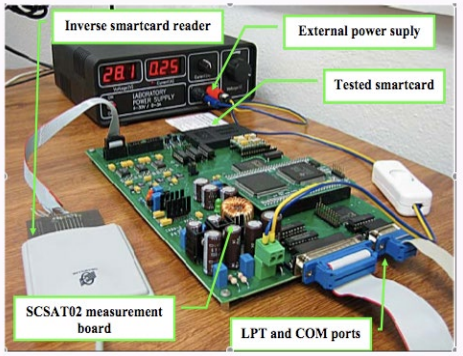
- Captured Drone by Iran

Counterfeit Integrated Circuits

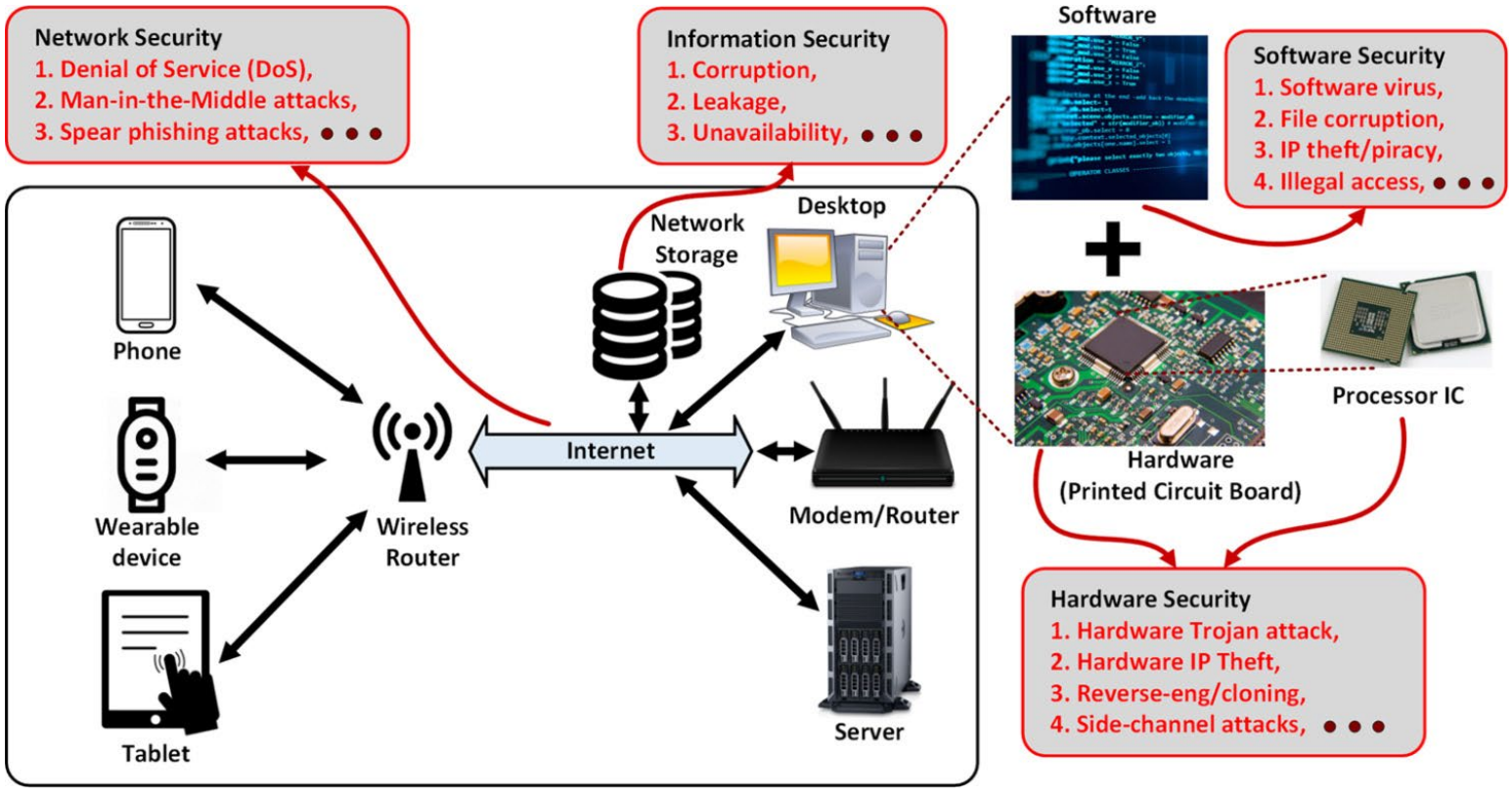
- Multi-billion dollar business



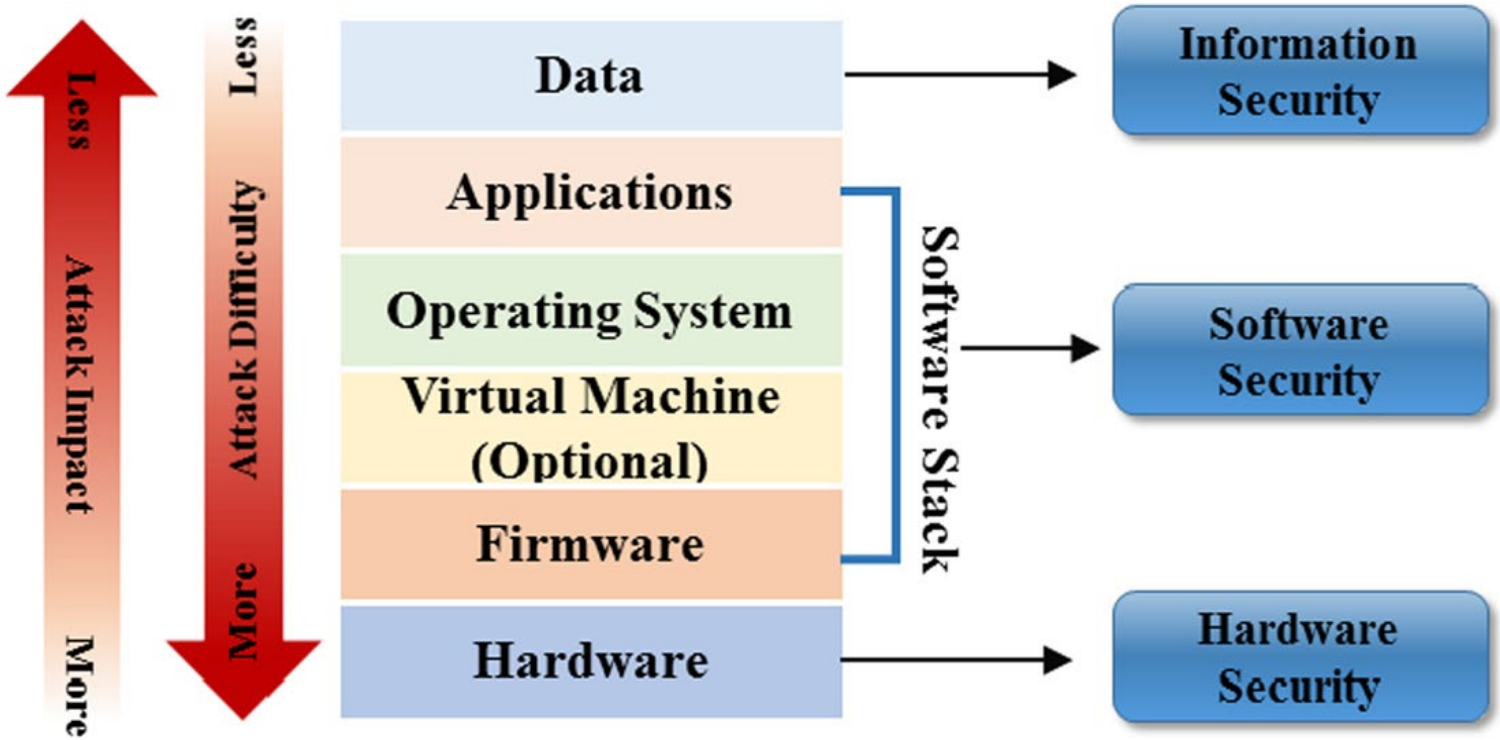




The landscape of Security in Modern Computing Systems

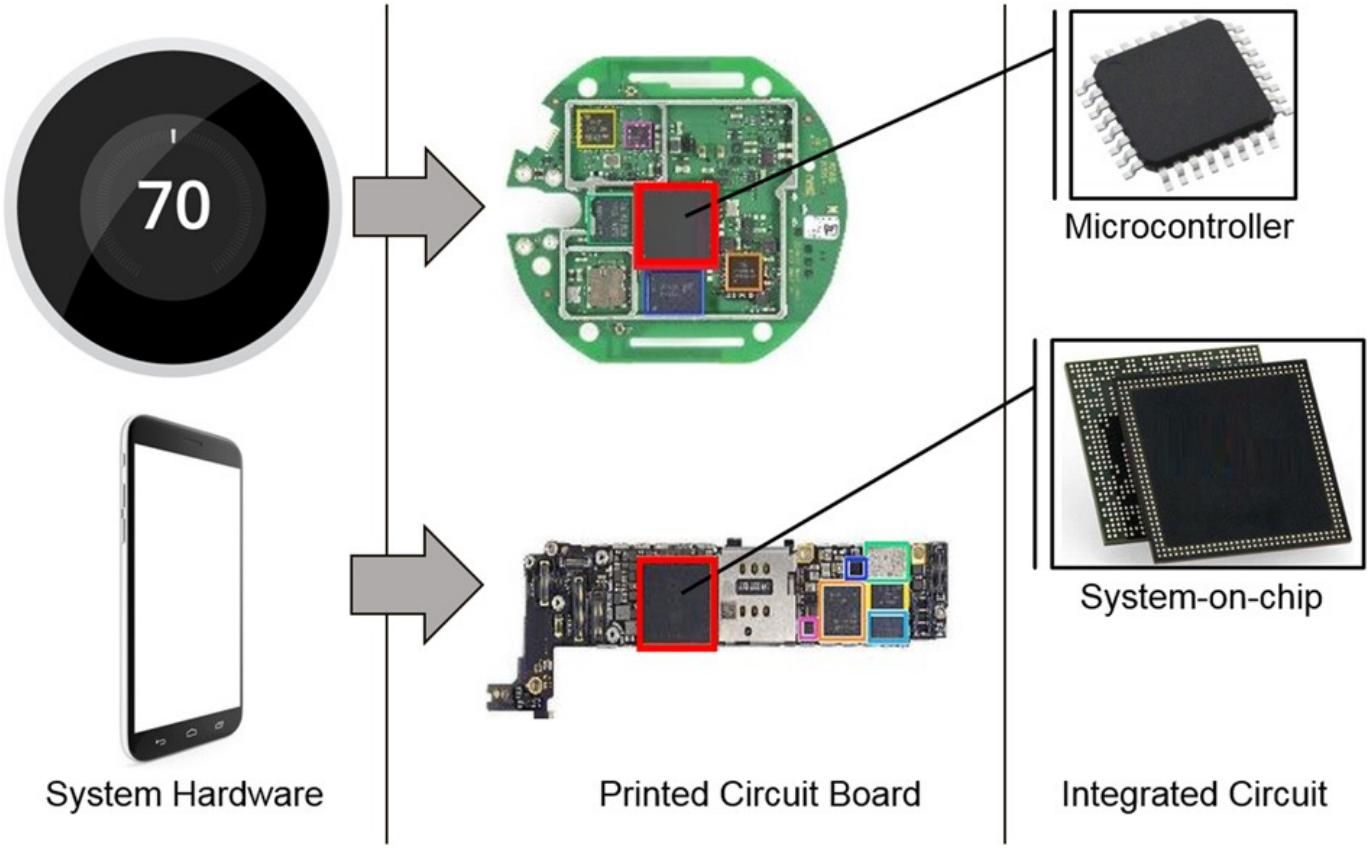


Attack impact and difficulty at different layers of a computing system

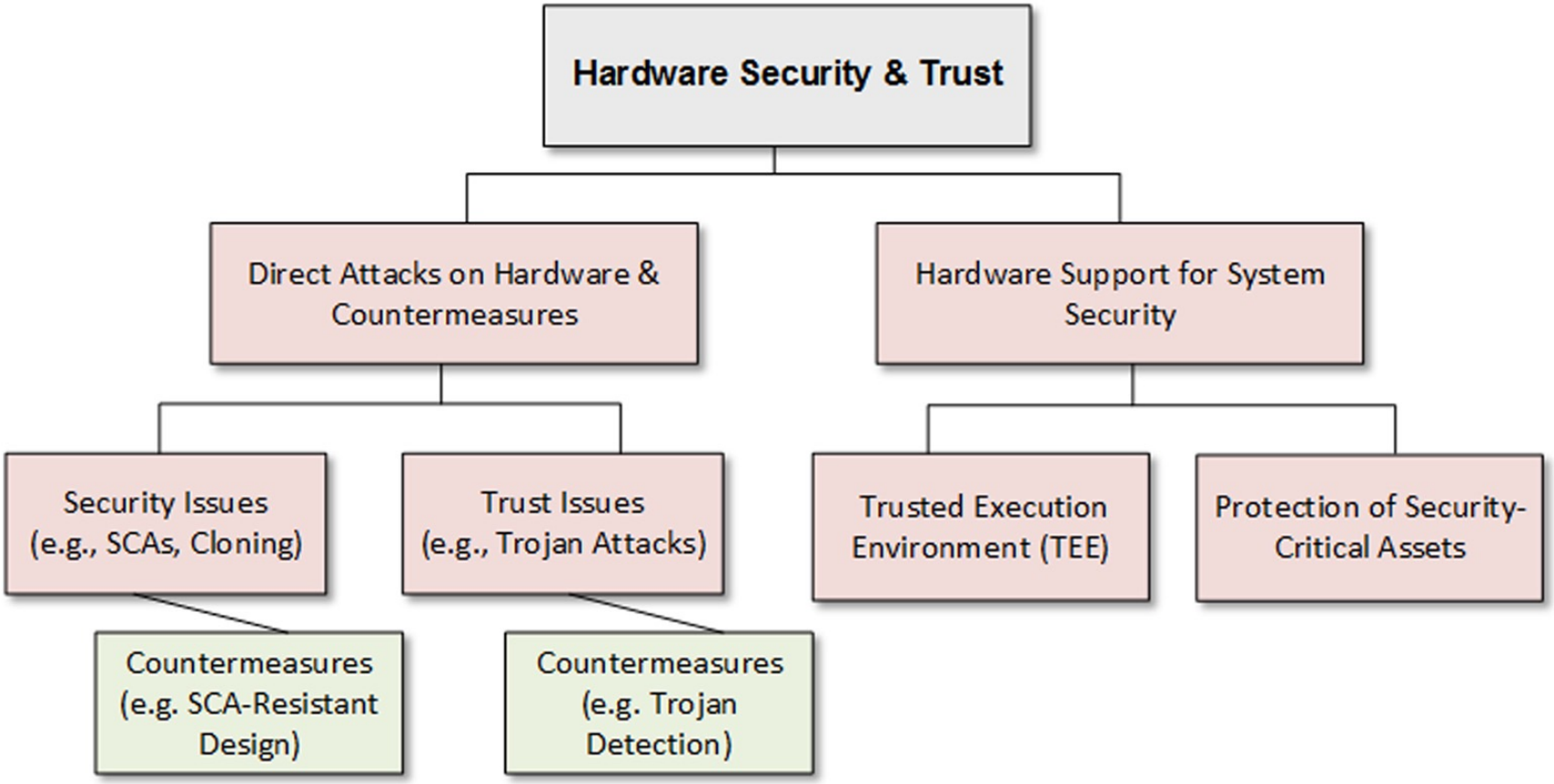


Modern Electronic Hardware

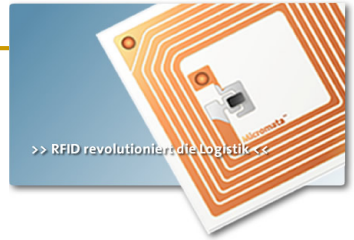
Three abstraction layers of modern electronic hardware (shown for two example devices)



Scope of hardware security and trust



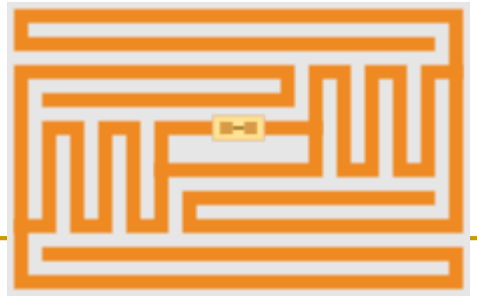
RFIDs



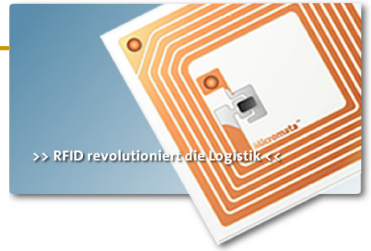
Radio-frequency identification (**RFID**) is the use of an object (typically referred to as an RFID tag) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

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



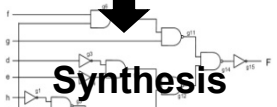
- Many applications in securing transactions,
  - Inventory Control Container / Pallet Tracking
  - ID Badges and Access Control
  - Fleet Maintenance Equipment/Personnel Tracking in Hospitals
  - Parking Lot Access and Control
  - Car Tracking in Rental Lots
  - Product Tracking through Manufacturing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

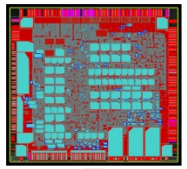
Evolution of Hardware Security and Trust

- **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…

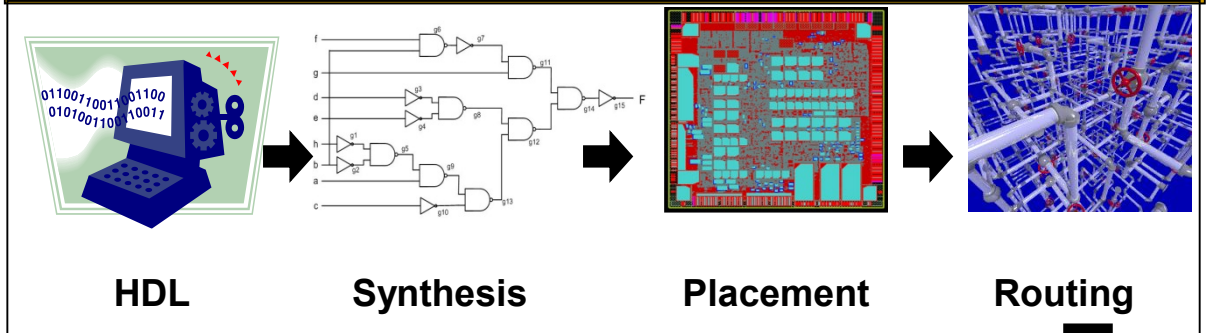
Shift in the Industry's Business Model

Vertical - one company



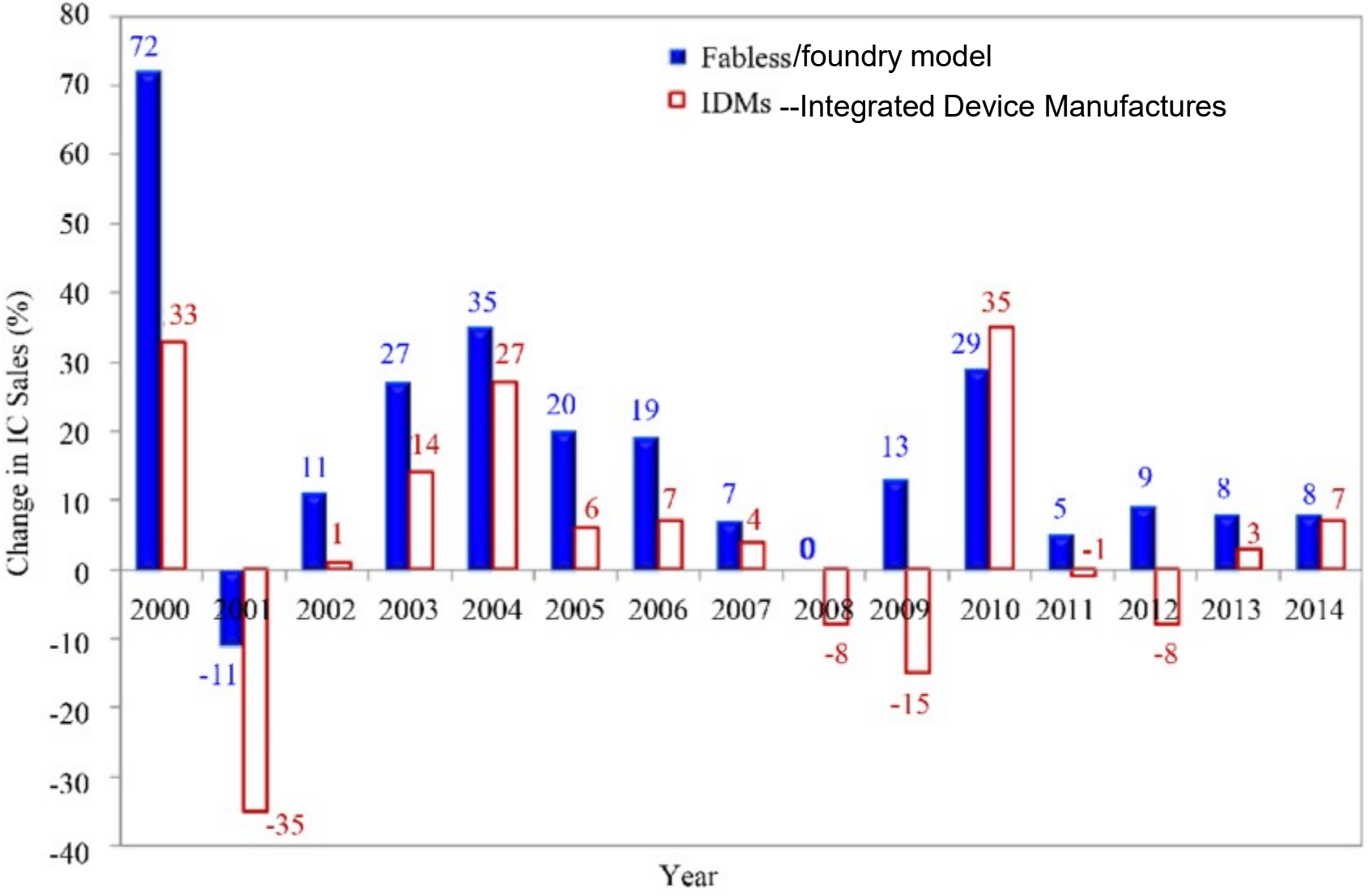


Horizontal (Dominant) – Two or more companies

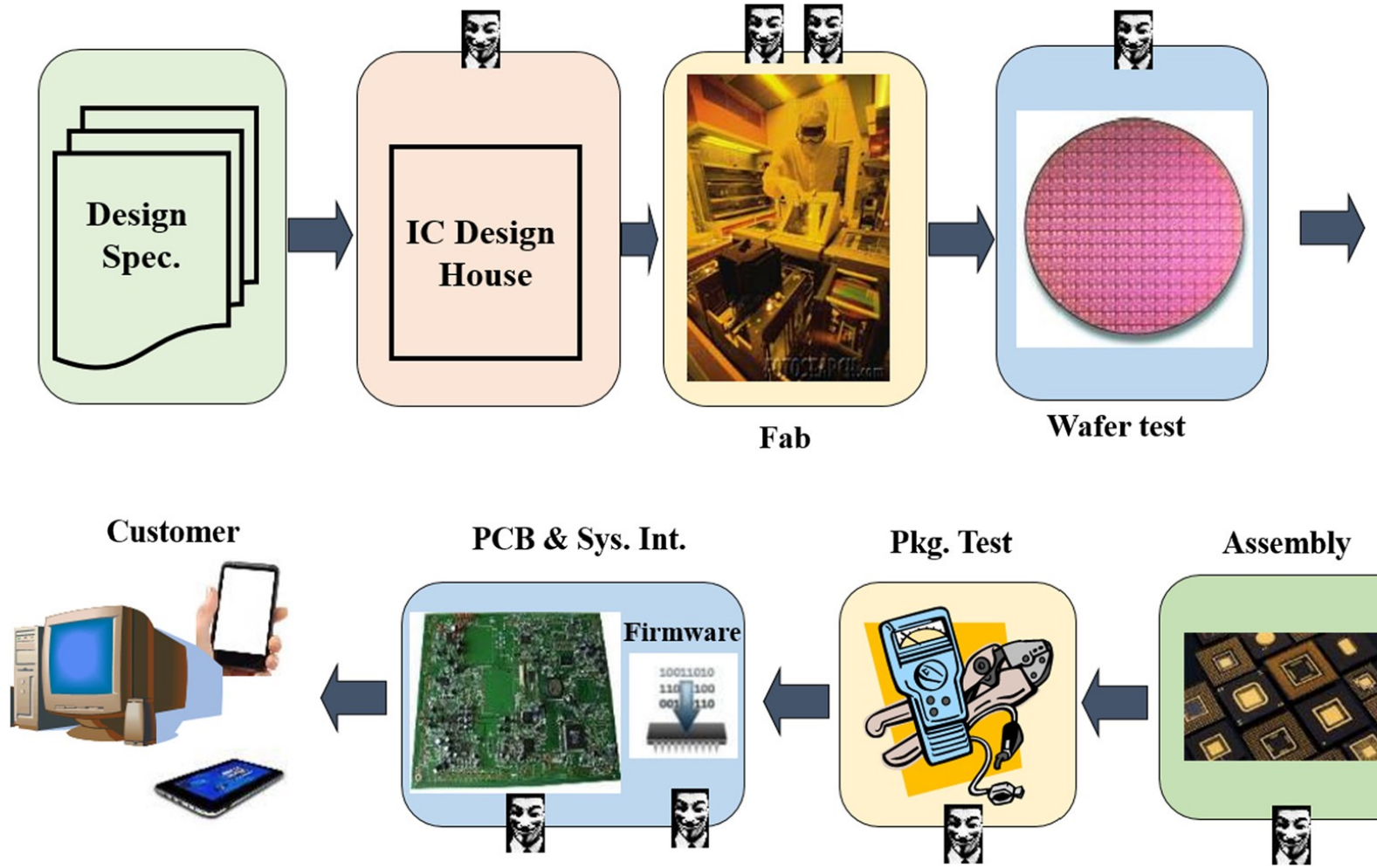


Economy of scale:
The same fabrication facility serves many fabless companies

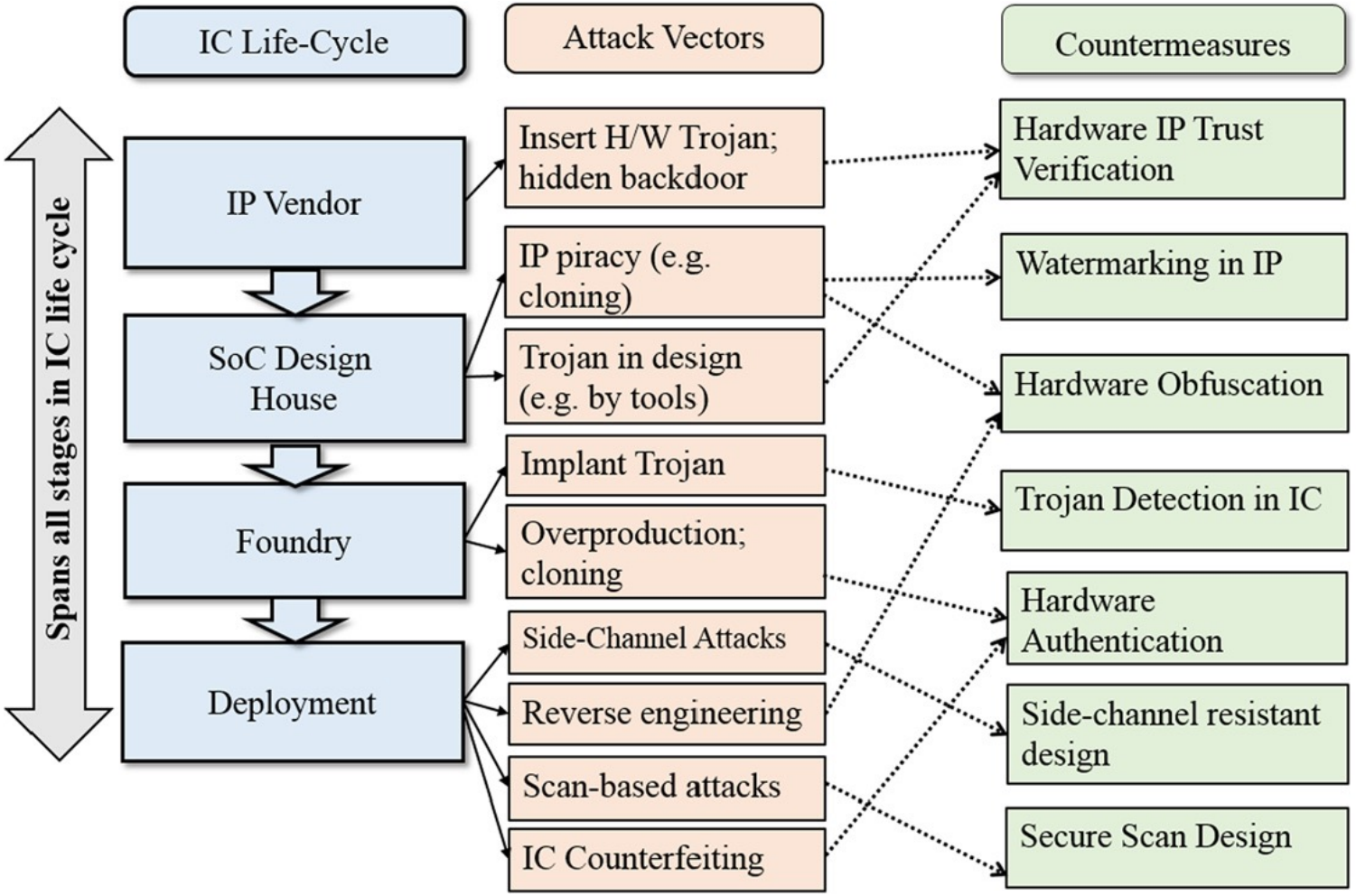
Microelectronic Industry Business Model



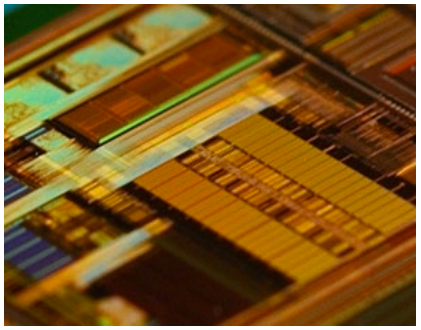
Major steps in the electronic hardware design and test flow

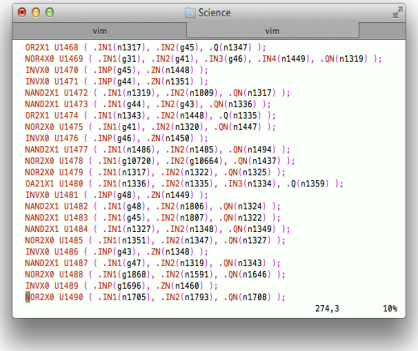


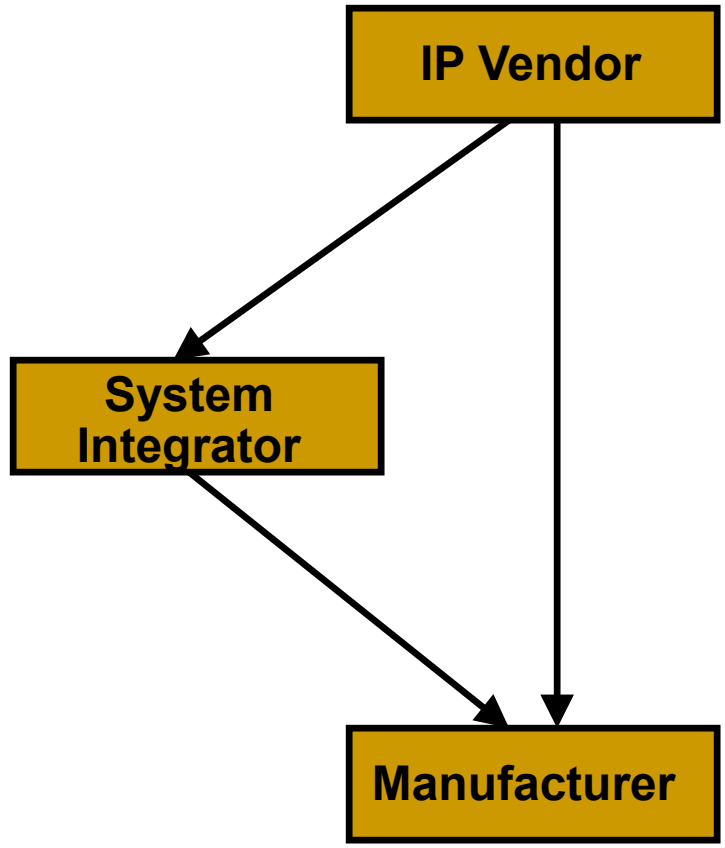
Attack vectors and countermeasures



HW Threats

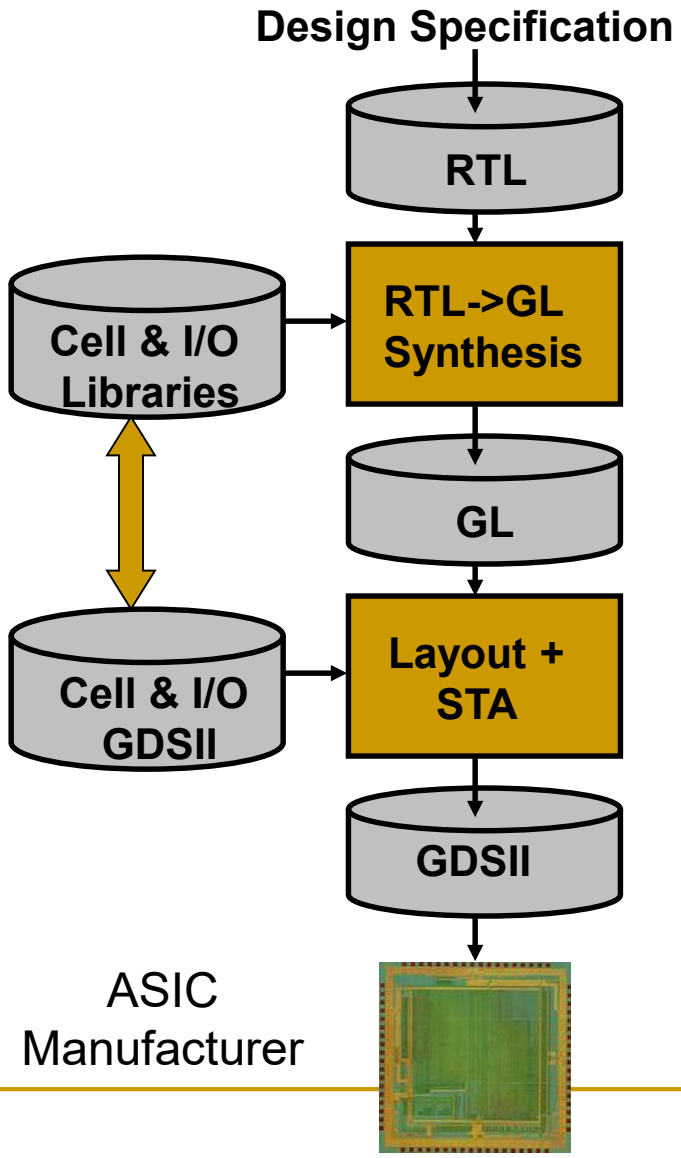






Any of these steps can be untrusted

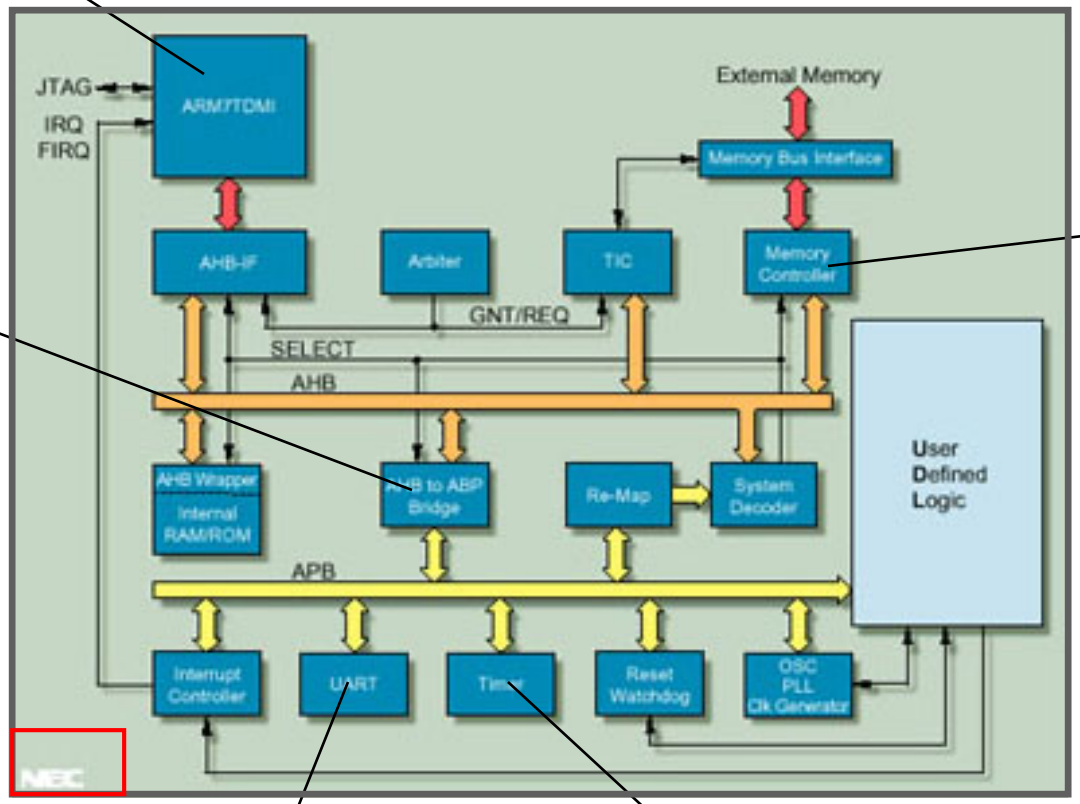
Design Process – Old Way



Design Process--New Way

Company X

System-on-Chip (SoC)



Company Y

Company Z

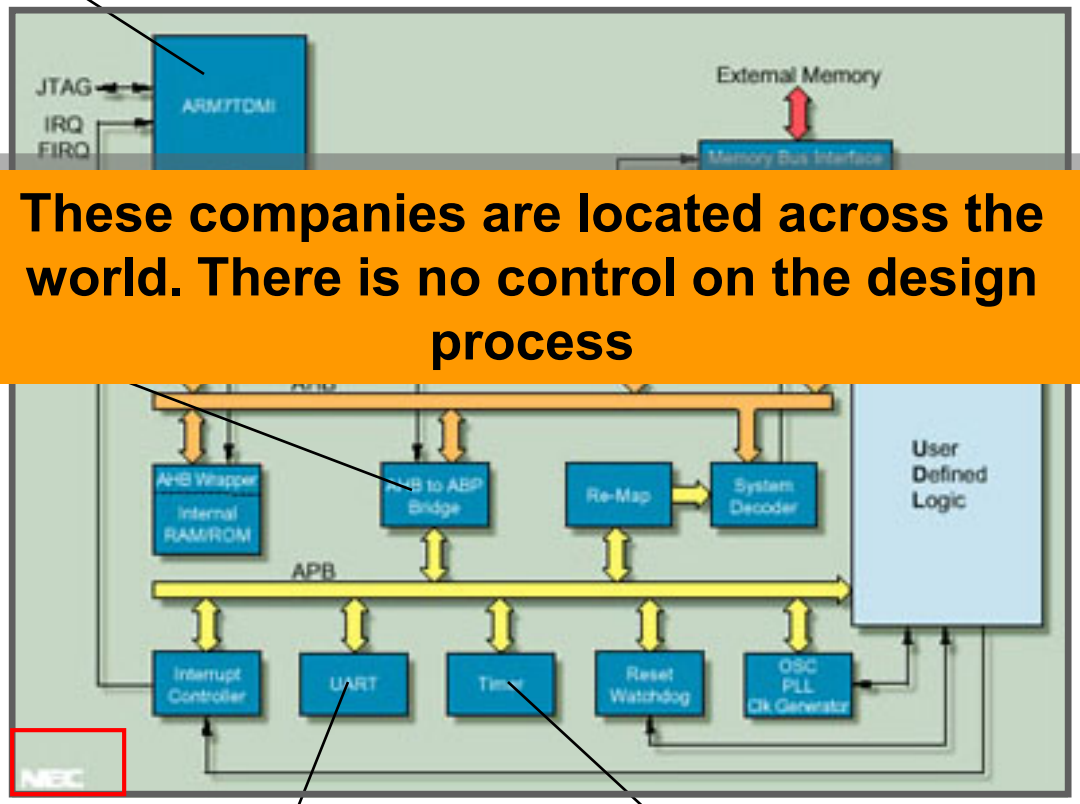
Company V

Company W

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

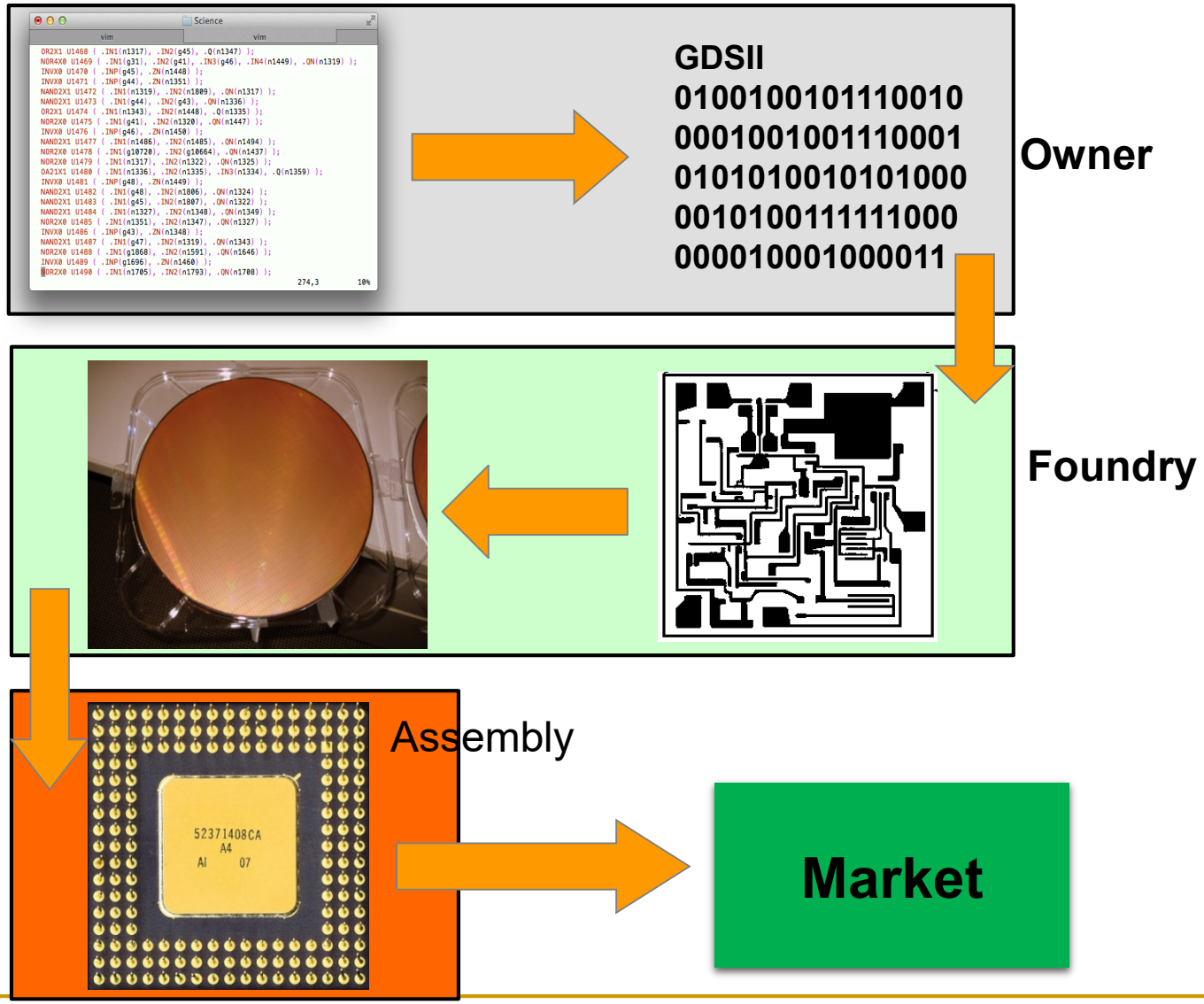
Company V

Company W

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

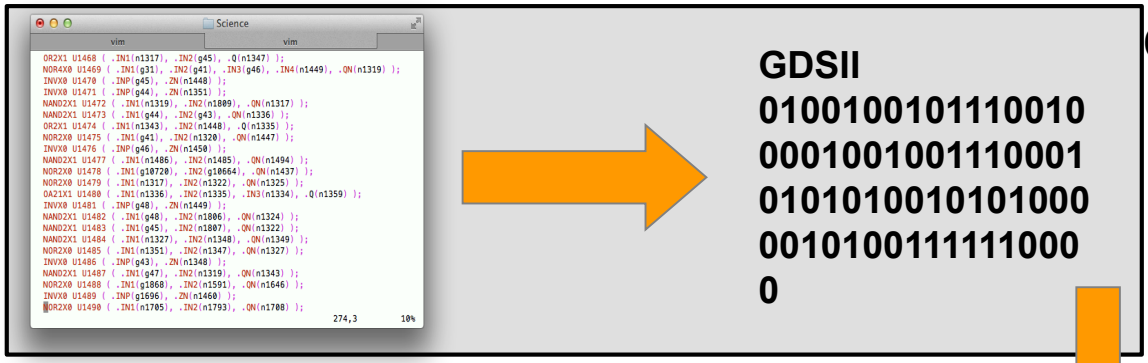
Who Develops the IPs? Who Designs the ICs? Who Fabricates Them?

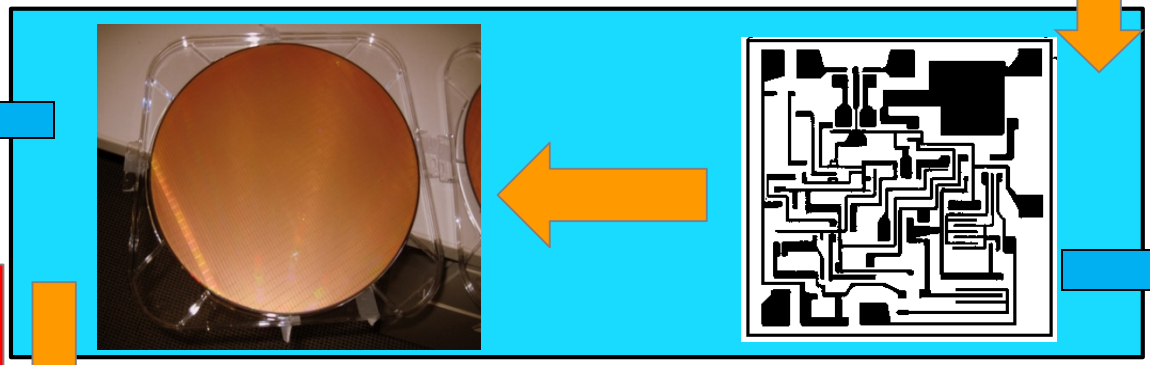
Counterfeiting—Original Design Process



Google image

Counterfeiting

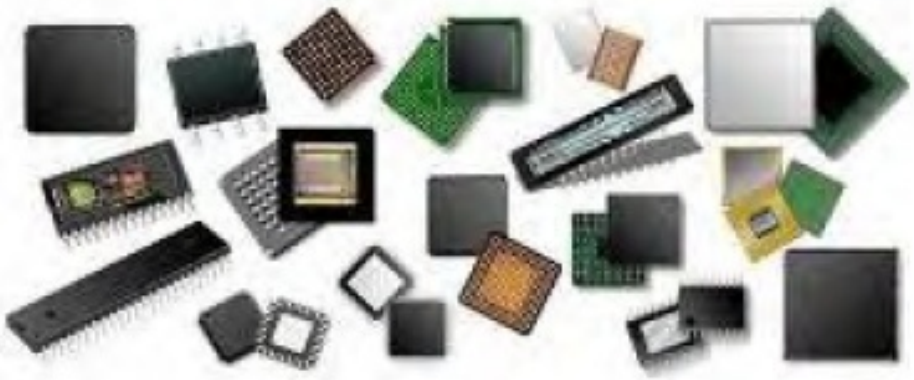




Google image

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

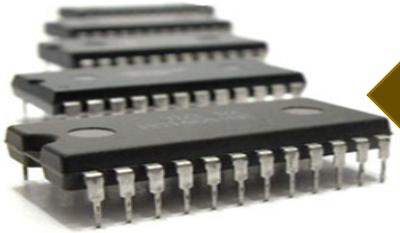
A recycling center

PCBs taken off of electronic systems

ICs taken off of PCBs

Refine recycled ICs

Resold as new



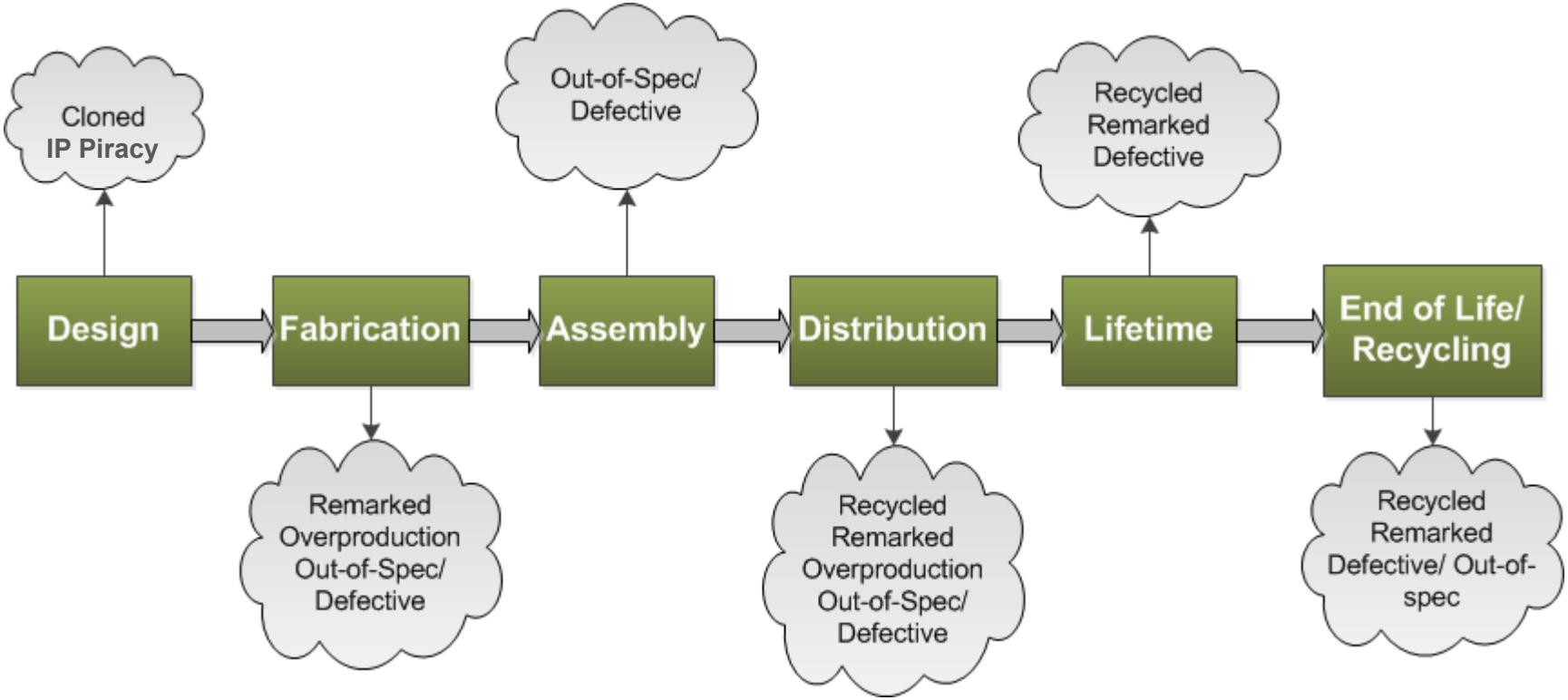
Critical Application

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



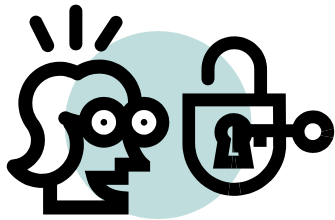
Some Basic Definitions

- **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"…



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.

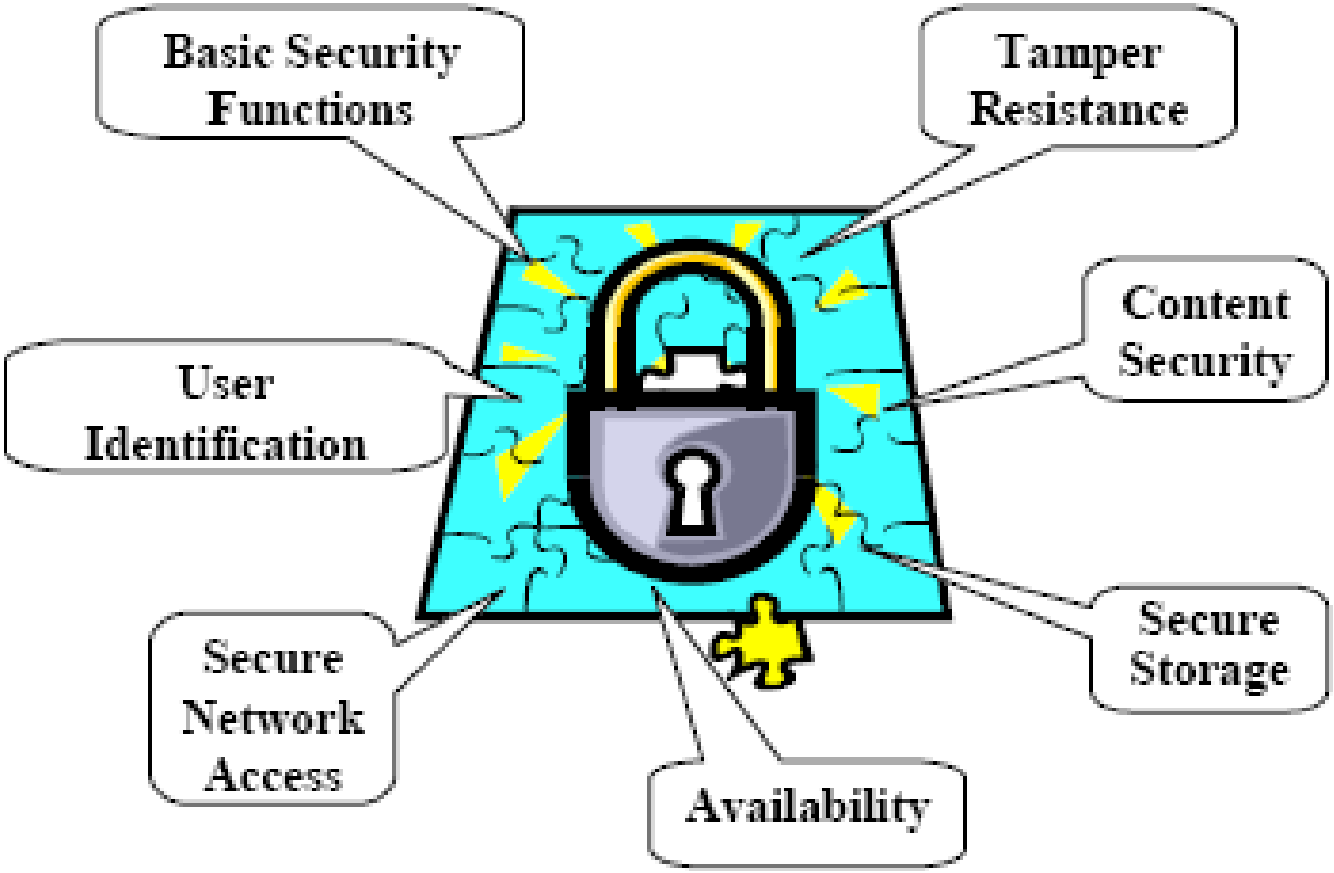
Hardware Controls for Secure Systems

- 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

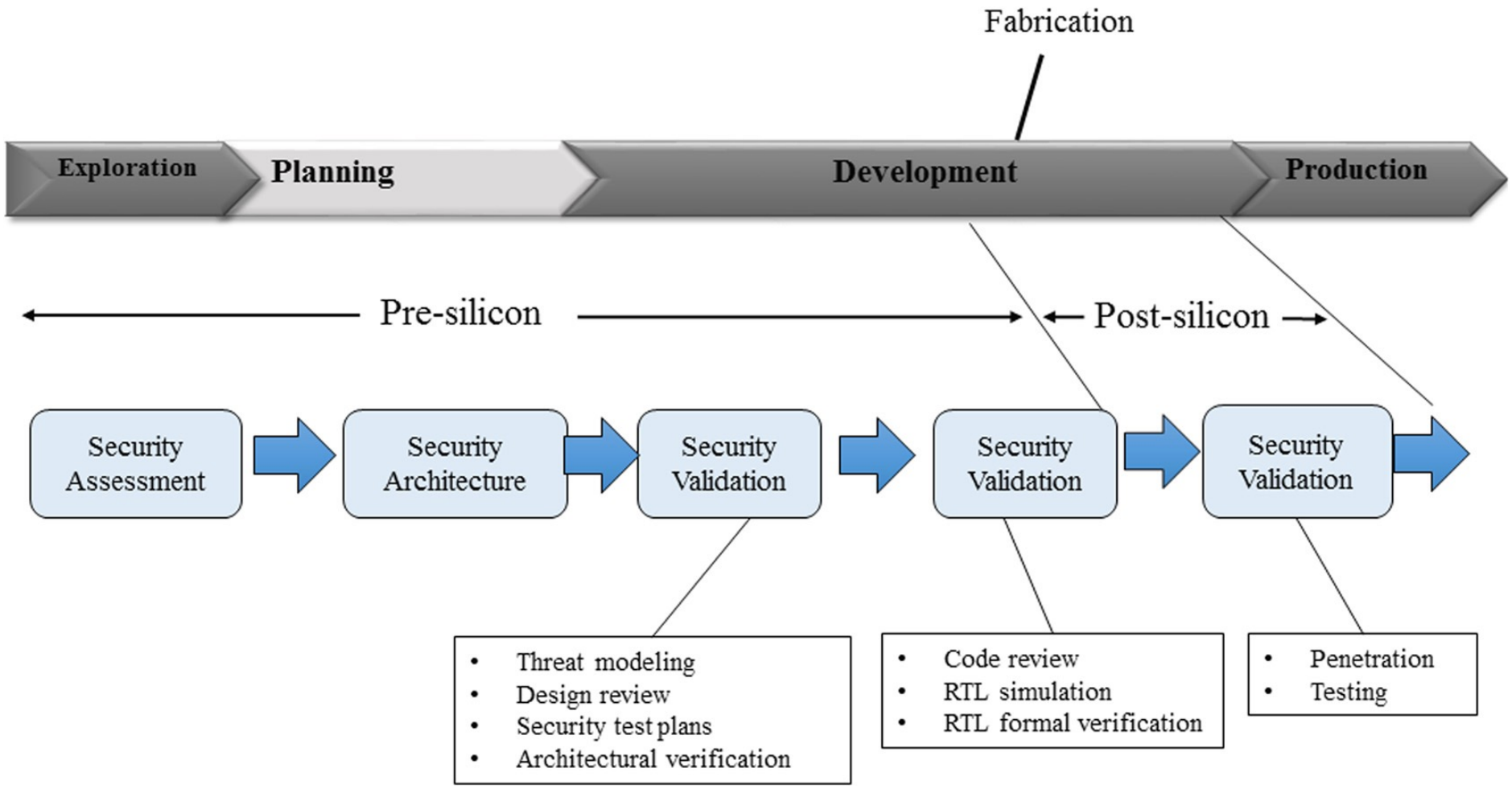
- Security processing adds overhead
  - Performance and power
- Security is challenging in embedded systems/IoTs
  - Size and power constraints, and operation in harsh environments
- Security processing may easily overwhelm the other aspects of the system
- Security has become a new design challenge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

Security Requirements in the IoT Era



Possible attack surfaces in a computing system

State of the practice in security design and validation along the life cycle of a system on chip.



Secret

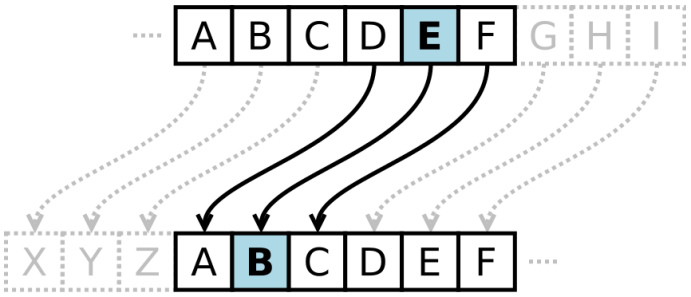
- **Underlying most security mechanisms or protocols is the notion of a "secret"**
  - Lock and keys
  - Passwords
  - Hidden signs and procedures
  - Physically hidden

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

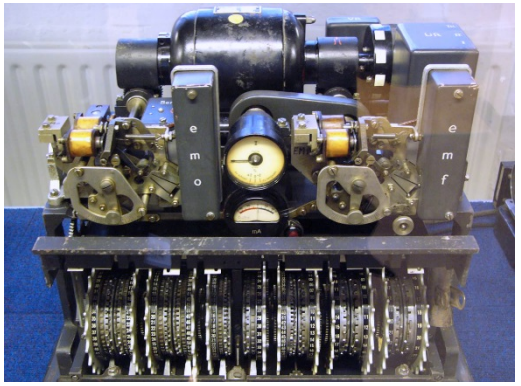
- Cryptoquote: simple substitution cipher, permutations of 26 letters
  - Using the dictionary and the frequencies, this is also easy to break

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!



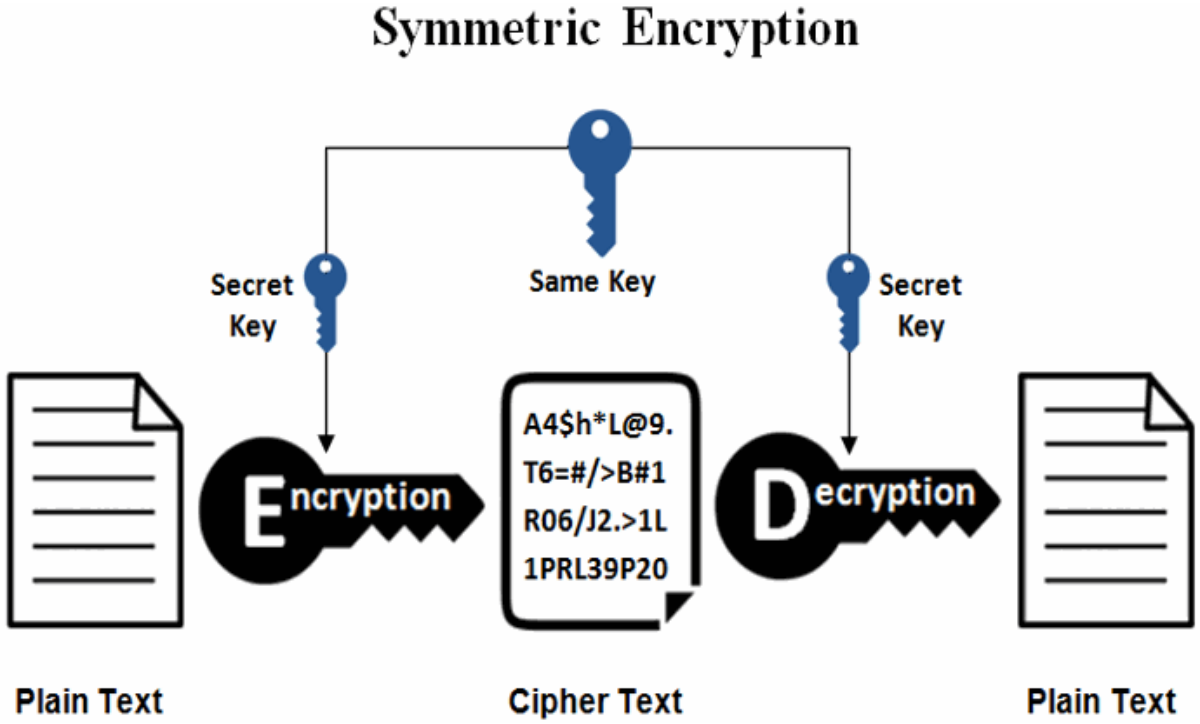
German rotor stream cipher machines used by the German Army during World War II

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
  - AES: Advanced Encryption Standard

DES

- DES is a symmetric-key algorithm for the encryption of digital data.

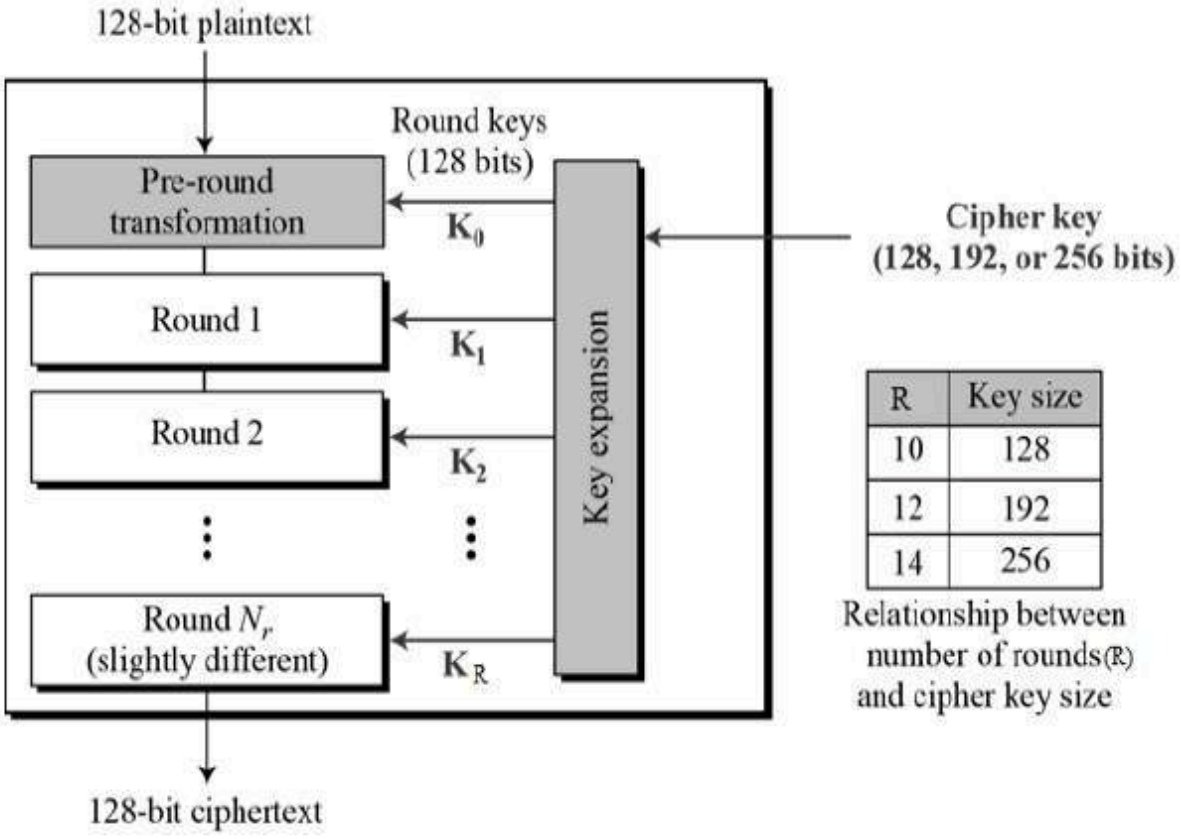


AES

- DES is insecure for modern applications due to the relatively short 56-bit key size.
- AES was established by the U.S. NIST in 2001.
- AES
  - Plaintext – 128 bits
  - Key – 128, 192, 256 bits

AES

- Blocks of information are shuffled through multiple rounds for bit shifting, swapping and multiplying.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds (R) and cipher key size