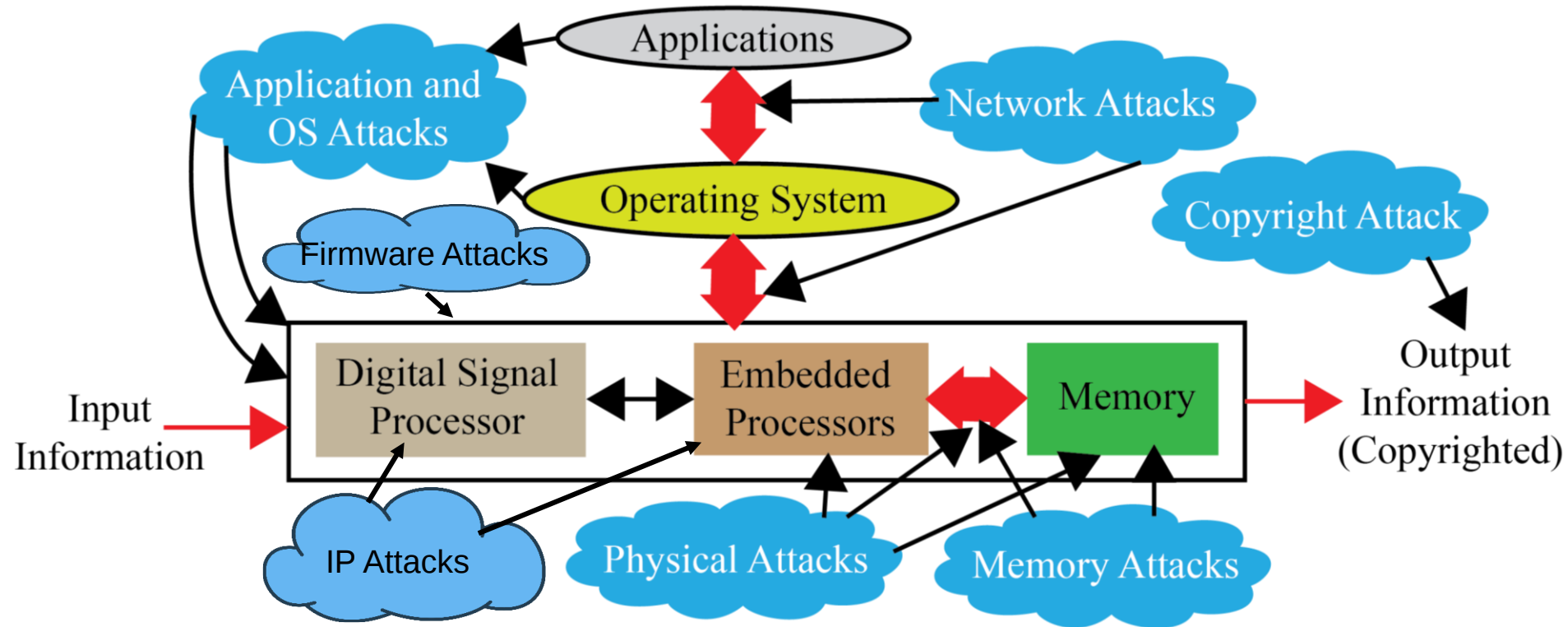

Energy and Security Tradeoffs in CE Systems

Saraju P. Mohanty
University of North Texas, USA.

Email: saraju.mohanty@unt.edu
More Info: <http://www.smohanty.org>



Selected Attacks on a Typical CE System – Security, Privacy, IP Right



Diverse forms of Attacks, following are not the same: System Security, Information Security, Information Privacy, System Trustworthiness, Hardware IP protection, Information Copyright Protection.

CE System Security – Smart Car

Protecting Communications

Particularly any Modems for In-vehicle Infotainment (IVI) or in On-board Diagnostics (OBD-II)

Over The Air (OTA) Management
From the Cloud to Each Car

Cars can have 100 Electronic Control Units (ECUs) and 100 million lines of code, each from different vendors – Massive security issues.

Protecting Each Module

Sensors, Actuators, and Anything with an Microcontroller Unit (MCU)

Mitigating Advanced Threats
Analytics in the Car and in the Cloud

- Connected cars require latency of ms to communicate and avoid impending crash:
 - ❑ Faster connection
 - ❑ Low latency
 - ❑ Energy efficiency

Security Mechanism Affects:

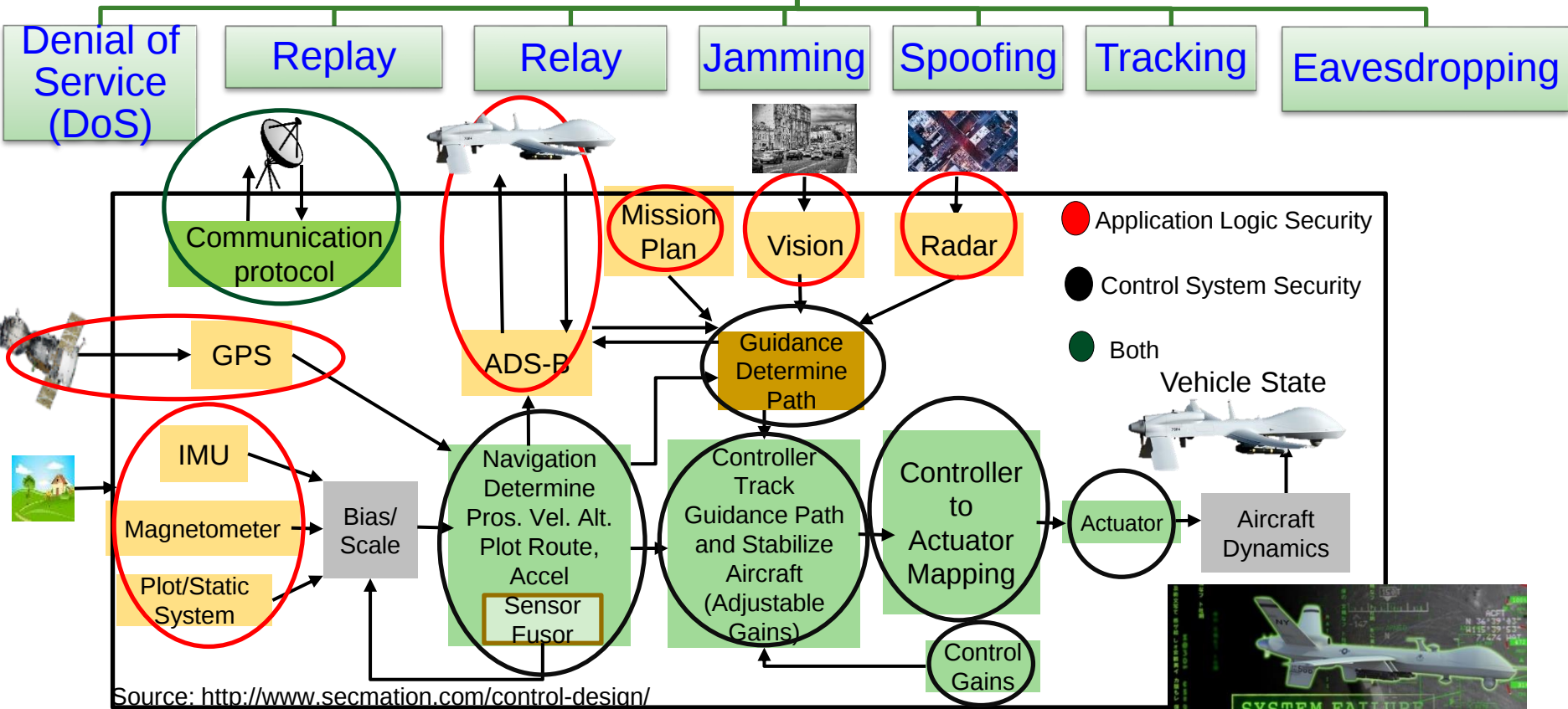
- Latency
- Mileage
- Battery Life

Source: http://www.symantec.com/content/en/us/enterprise/white_papers/public-building-security-into-cars-20150805.pdf



CE System Security – UAV

Selected Attacks on UAV



Security Mechanisms Affect:

Battery Life Latency Weight Aerodynamics



Source: <http://politicalblindspot.com/u-s-drone-hacked-and-hijacked-with-ease/>



Smart Healthcare - Security and Privacy Issue



Selected Smart Healthcare Security/Privacy Challenges

Data Eavesdropping

Data Confidentiality

Data Privacy

Location Privacy

Identity Threats

Access Control

Unique Identification

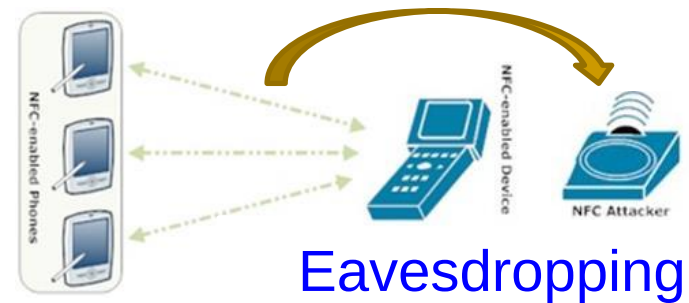
Data Integrity

NFC Security - Attacks

Selected NFC Attacks



Source: <http://www.idigitaltimes.com/new-android-nfc-attack-could-steal-money-credit-cards-anytime-your-phone-near-445497>



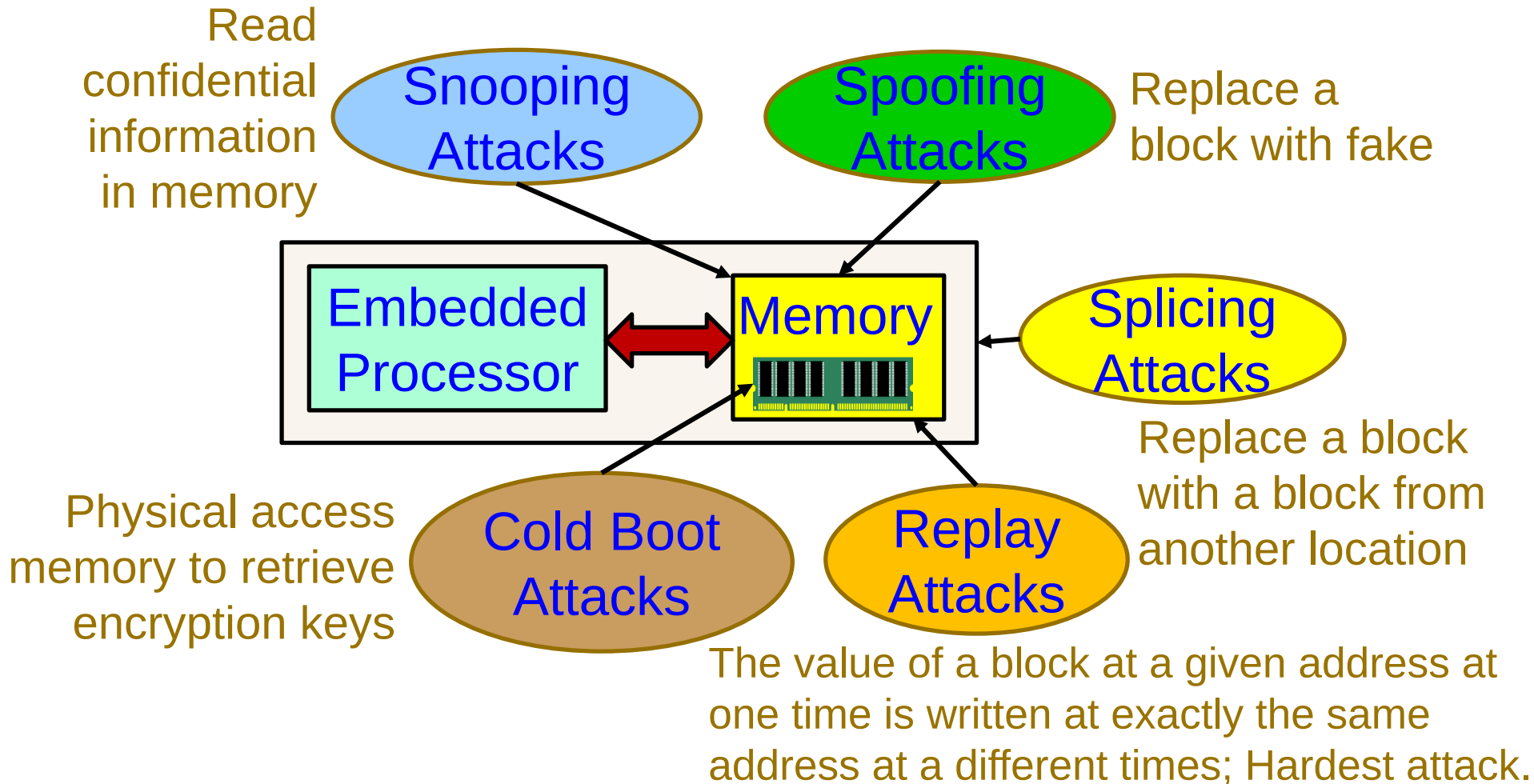
Source: <http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/>



Source: <https://www.slideshare.net/cgwzq/on-relaying-nfc-payment-transactions-using-android-devices>



Memory Attacks



Source: Mohanty 2013, Springer CSSP Dec 2013

Counterfeit Hardware – IP Attacks

2014 Analog Hardware Market (Total Shipment Revenue US \$)



Wireless Market
\$18.9 billion (34.8%)



Consumer Electronics
\$9.0 billion (16.6%)



Industrial Electronics
\$8.9 billion (16.5%)



Automotive
\$8.5 billion (15.7%)



Data Processing
\$6.0 billion (11%)



Wired Communications
\$2.9 billion (5.4%)

Source: <https://www.slideshare.net/rorykingihs/ihs-electronics-conference-rory-king-october>

Top counterfeits could have impact of
\$300B on the semiconductor market.



Attacks - Software Vs Hardware

Software Based

- Software attacks via communication channels
- Typically from remote
- More frequent
- Selected Software based:
 - ❑ Denial-of-Service (DoS)
 - ❑ Routing Attacks
 - ❑ Malicious Injection
 - ❑ Injection of fraudulent packets
 - ❑ Snooping attack of memory
 - ❑ Spoofing attack of memory and IP address
 - ❑ Password-based attacks

Hardware Based

- Hardware or physical attacks
- Maybe local
- More difficult to prevent
- Selected Hardware based:
 - ❑ Hardware backdoors (e.g. Trojan)
 - ❑ Inducing faults
 - ❑ CE system tampering/jailbreaking
 - ❑ Eavesdropping for protected memory
 - ❑ Side channel attack
 - ❑ CE hardware counterfeiting



Security - Software Vs Hardware

Software Based

- Flexible - Easy to use, upgrade and update
- Wider-Use - Use for all devices in an organization
- Higher recurring operational cost
- Tasks of encryption easy compared to hardware – substitution tables
- Needs general purpose processor
- Can't stop hardware reverse engineering

Hardware Based

- High-Speed operation
- Energy-Efficient operation
- Low-cost using ASIC and FPGA
- Tasks of encryption easy compared to software – bit permutation
- Easy integration in CE systems
- Possible security at source-end like sensors, better suitable for IoT
- Susceptible to side-channel attacks
- Can't stop software reverse engineering

Maintaining of Security of Consumer Electronics, CE Systems, IoT, CPS, etc. needs Energy and affects performance.



Hardware Assisted Security

- Software based Security:
 - ❑ A general purposed processor is a deterministic machine that computes the next instruction based on the program counter.
 - ❑ Software based security approaches that rely on some form of encryption can't be full proof as breaking them is just matter of time.
 - ❑ It is projected that quantum computers that use different paradigms than the existing computers will make things worse.
- Hardware-Assisted Security: Security/Protection provided by the hardware: for information being processed by a CE system, for hardware itself, and/or for the CE system.



Hardware Assisted Security

- Hardware-Assisted Security: Security provided by hardware for:
 - (1) information being processed,
 - (2) hardware itself,
 - (3) overall system
- Additional hardware components used for security.
- Hardware design modification is performed.
- System design modification is performed.

RF Hardware Security

Digital Hardware Security – Side Channel

Hardware Trojan Protection

Information Security, Privacy, Protection

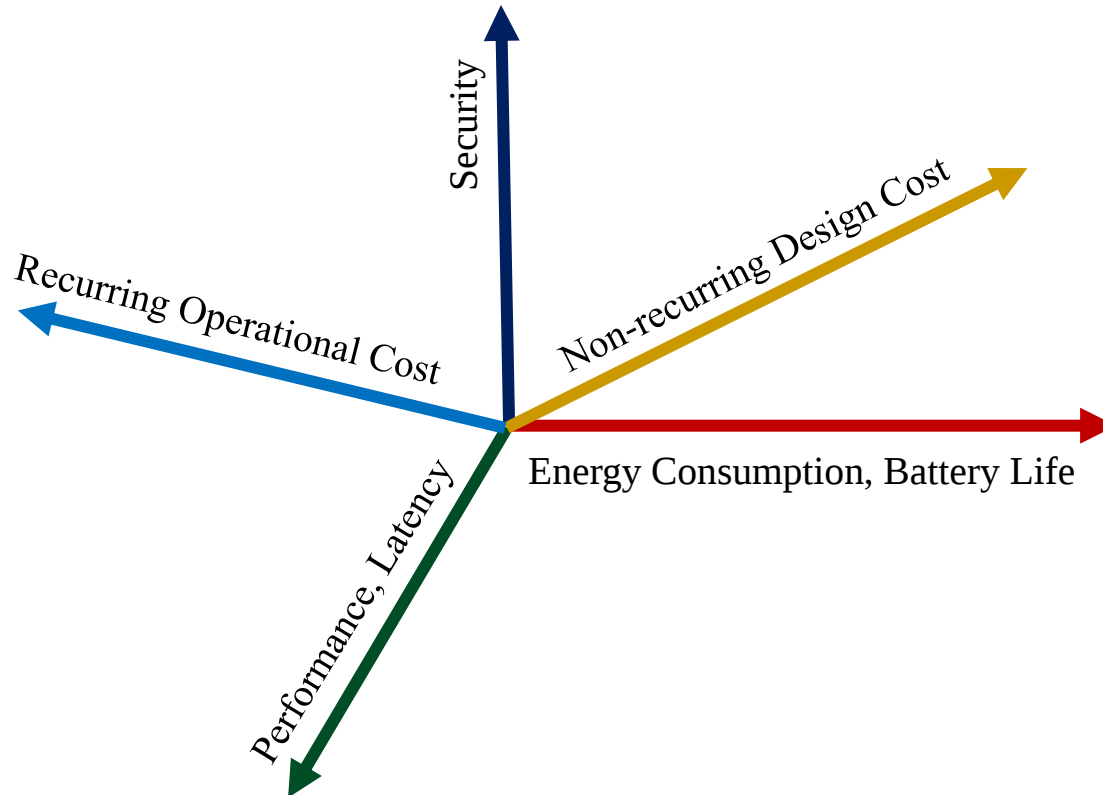
IR Hardware Security

Memory Protection

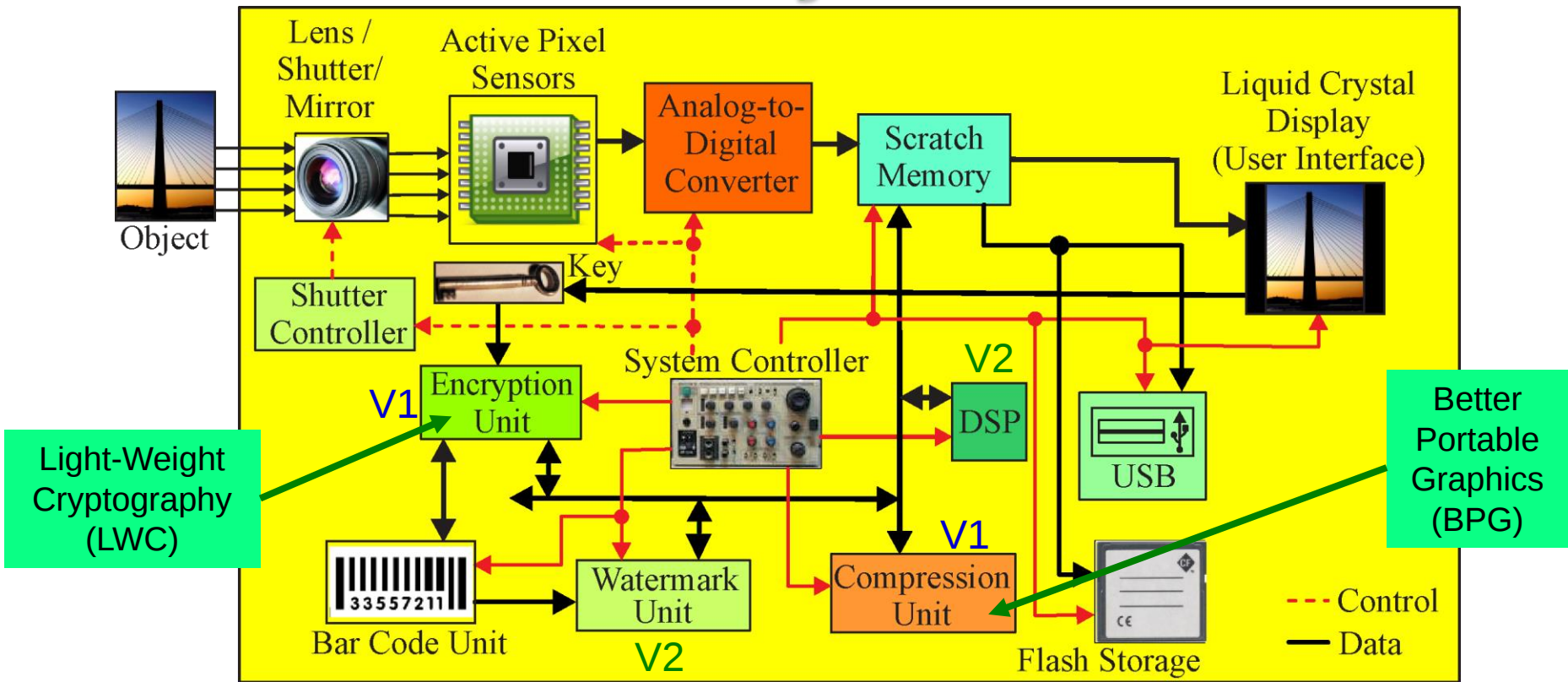
Digital Core IP Protection



CE System Design and Operation Tradeoffs



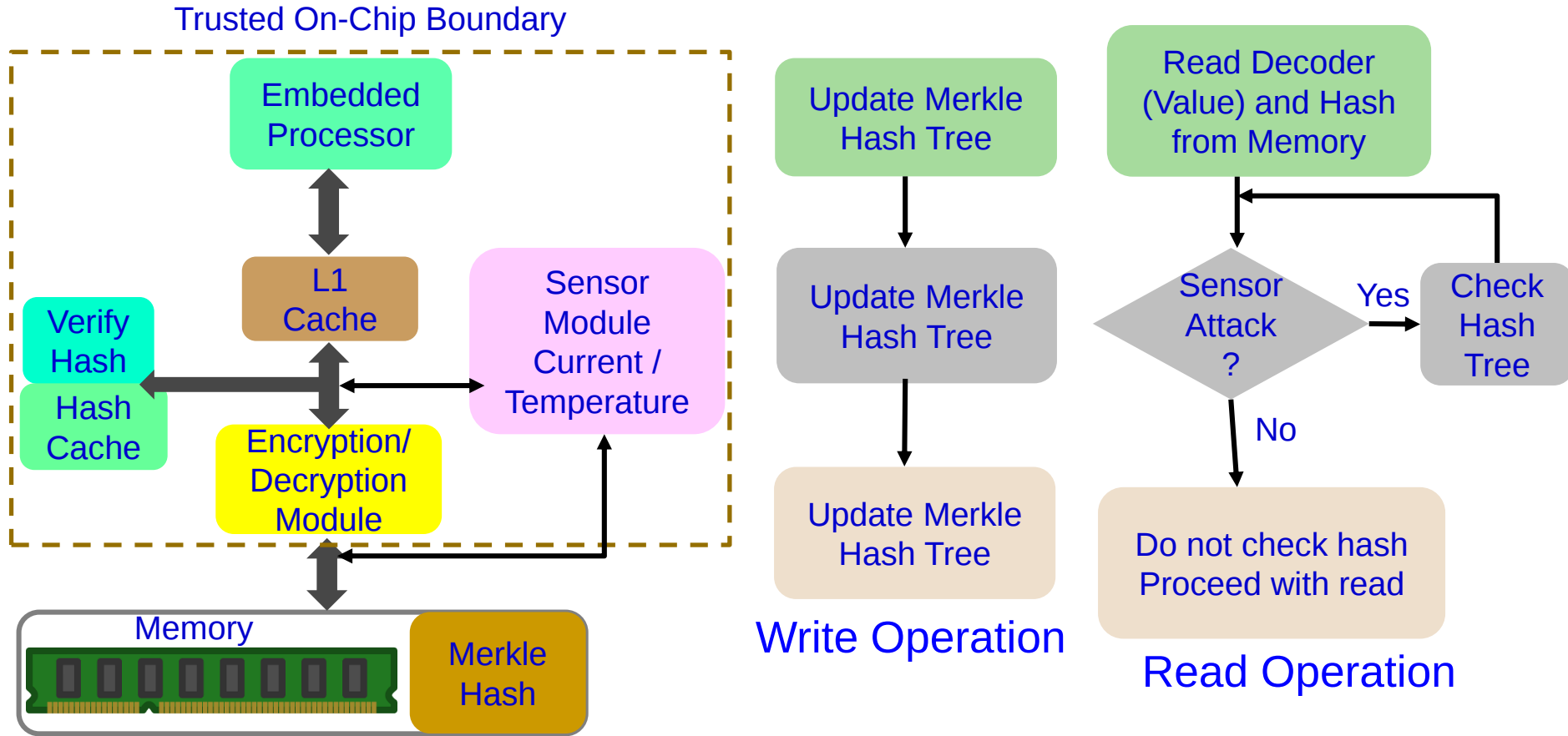
CE System Energy & Security Tradeoff – System Level



Include additional/alternative hardware/software components and uses DVFS like technology for energy and performance optimization.

Source: Mohanty 2006, TCAS-II May 2006; Mohanty 2009, JSA Oct 2009; Mohanty 2016, Access 2016

Embedded Memory Security and Protection

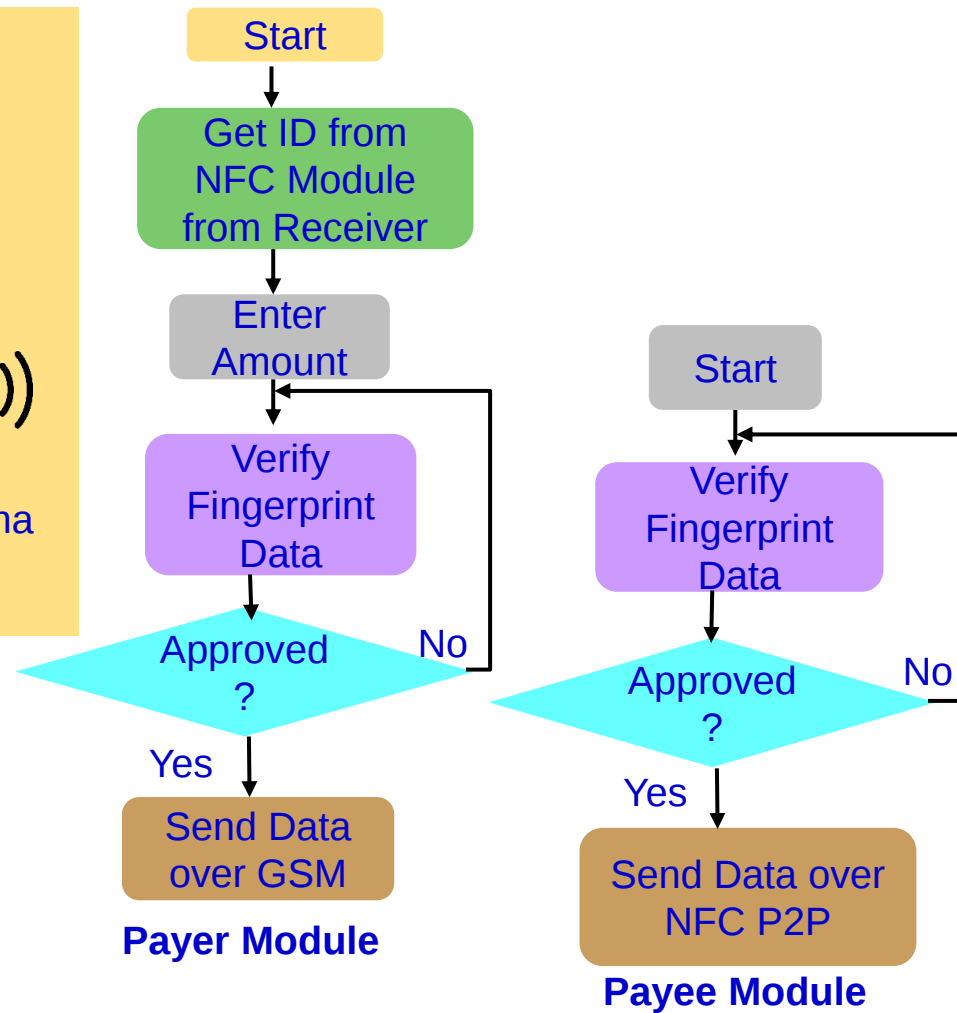
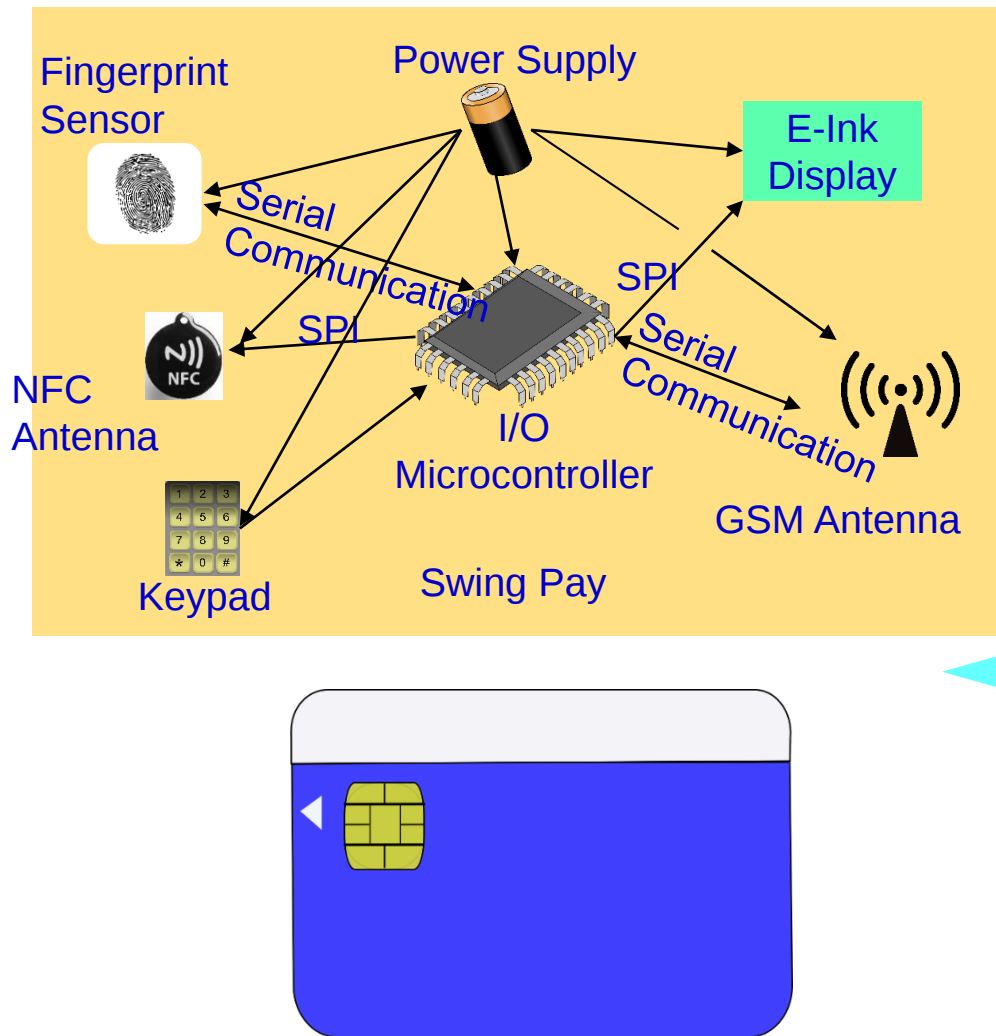


On-Chip/On-Board Memory Protection

Source: Mohanty 2013 and Springer CSSP Aug 2013



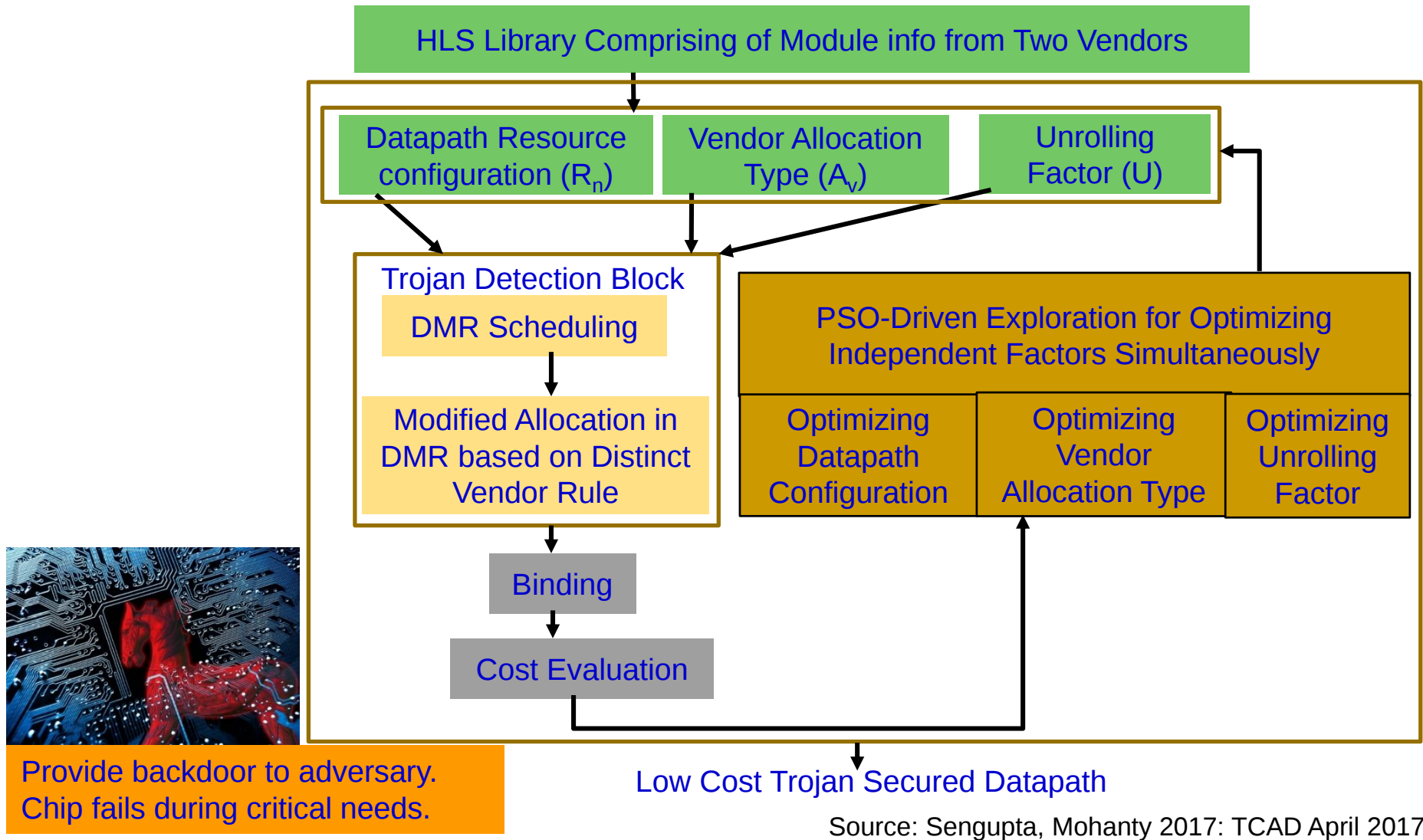
NFC Security



Source: Mohanty 2017, CE Magazine Jan 2017

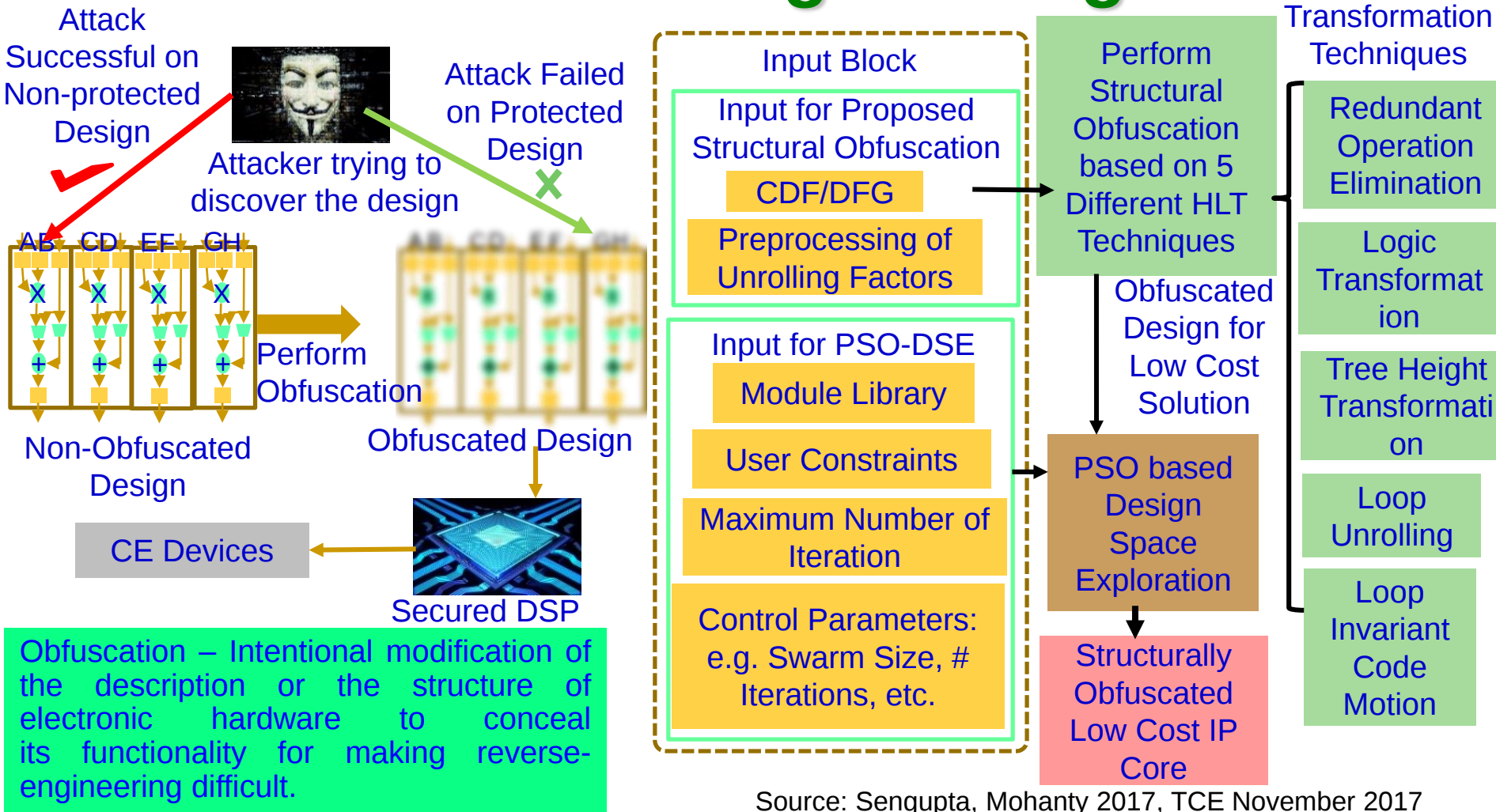


Trojan Secure Digital Hardware Synthesis



Source: Sengupta, Mohanty 2017: TCAD April 2017

Digital Hardware Synthesis to Prevent Reverse Engineering



Source: Sengupta, Mohanty 2017, TCE November 2017



Thank You !!!

Slides Available at: <http://www.smohanty.org>

Hardwares are the drivers of the civilization, even softwares need them.

