Special track
SCADD: Side Channel Attacks, Detection & Defenses

CYBER 2020
The 5th International Conference on Cyber-Technologies and Cyber-Systems

October 25-29, 2020 - Nice, French Riviera, France
https://www.iaria.org/conferences2020/CYBER20.html

INFORMATION TECHNOLOGY UNIVERSITY

cnrs

LIRMM

IARIA

Track Co-chairs

Khurram BHATTI
Associate Professor, Information Technology University,
Lahore, Pakistan
Khurram.bhatti@itu.edu.pk

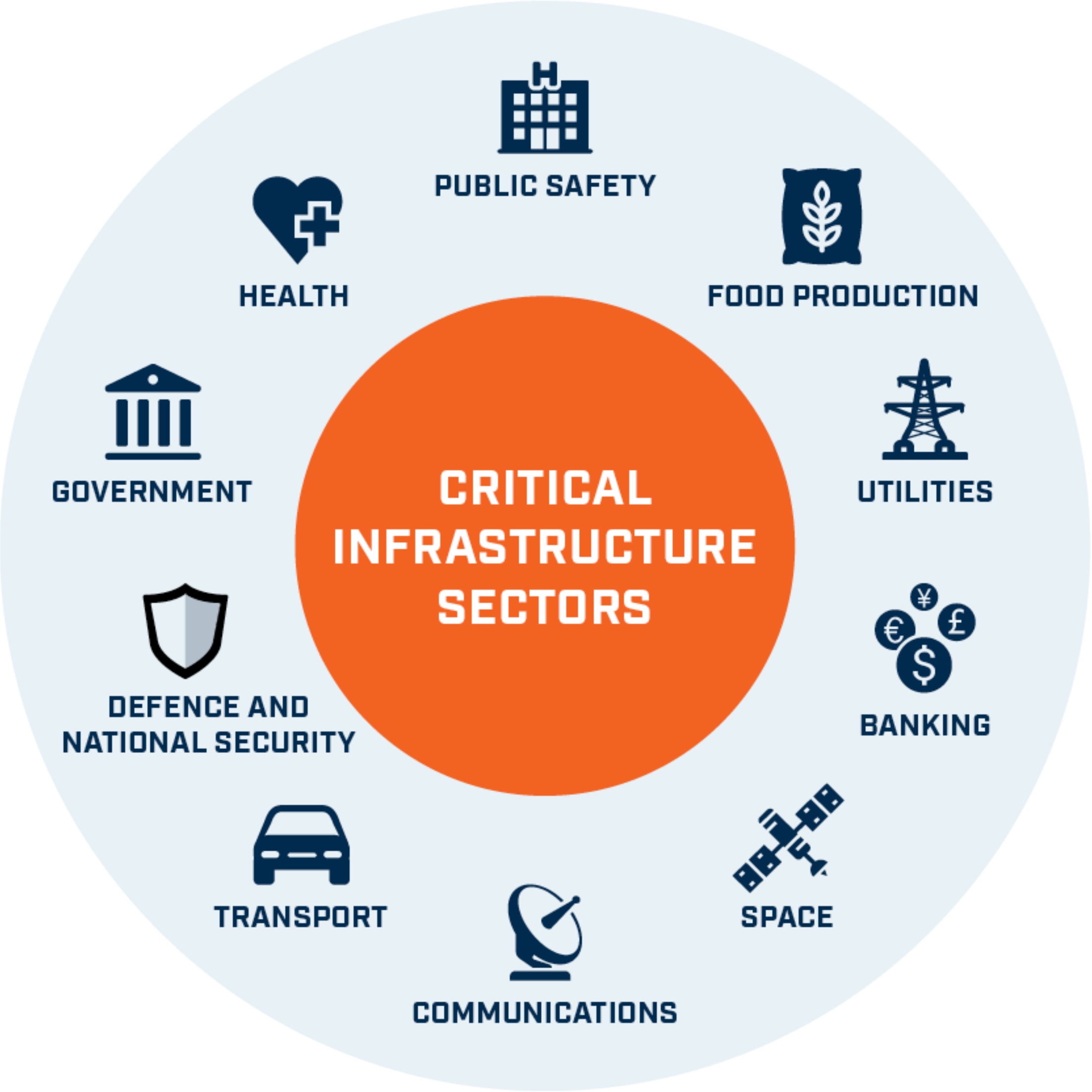
Khurram Bhatti is a Marie-Curie Research Fellow of KTH Royal Institute of Technology, Stockholm, for postdoc (2013-2014). His current research interests include embedded systems, information security at both hardware & software levels, Cryptanalysis, Mixed Criticality Systems and Parallel Computing Systems. Over the last 6 years, Khurram has taught at the University of Nice-Sophia Antipolis, France, and CIIT Lahore, Pakistan. He has been working with prestigious European research institutes like INRIA, Lab-STICC, KTH, École Polytechnique de Paris, and LEAT research laboratory. His research work has been published in international peer-reviewed journals and conferences. Khurram holds a PhD in Computer Engineering and MS in Embedded Systems from the University of Nice-Sophia Antipolis, France.

Maria MUSHTAQ
Scientific Researcher, LIRMM-CNRS, University of
Montpellier, France
Maria.mushtaq@lirmm.fr

Maria MUSHTAQ received her PhD in Information Security from the University of South Brittany (UBS), France, in 2019. She was awarded the French regional scholarship for her PhD. Currently, she is working as a CNRS Postdoctoral Researcher at LIRMM, University of Montpellier (UM), France under “excellence post-doc grant”. She possess expertise in microarchitectural vulnerability assessment and design & development of runtime mitigation solutions against side- and covert-channel information leakage in modern computing systems. Her research interests mainly focus on cryptanalysis, constructing and validating software security components, and constructing OS-based security primitives against various hardware vulnerabilities. She holds Masters and Bachelor's degrees in Computer Science.

Information Security

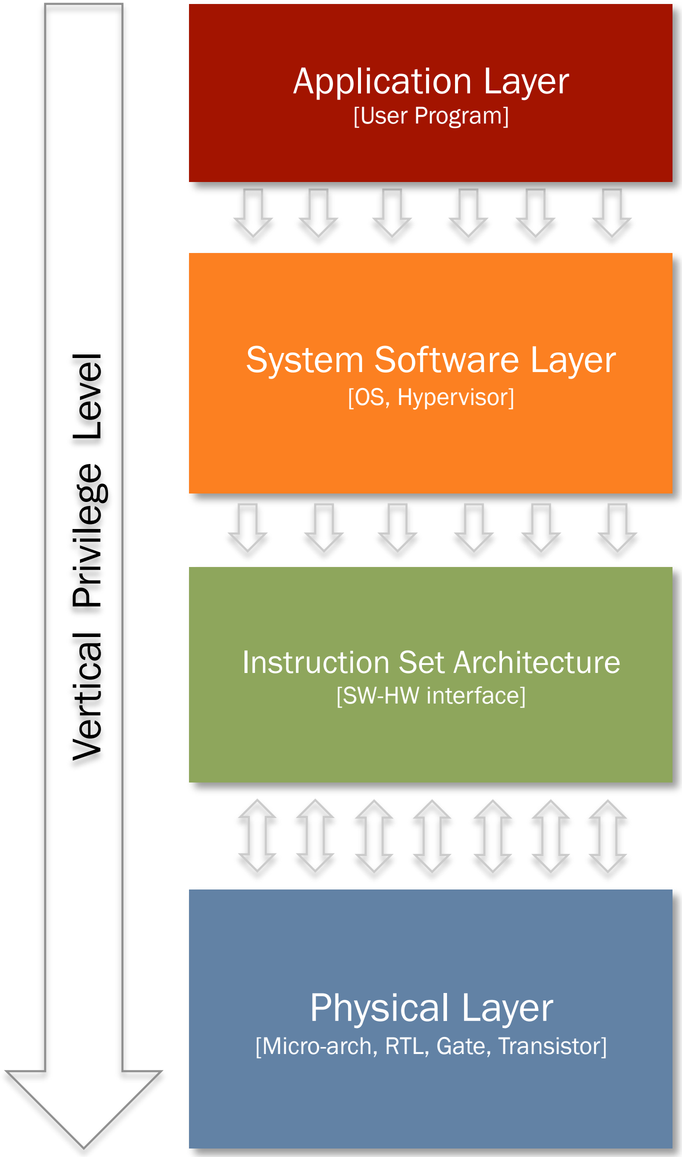
A shared concern by many application domains



Information Security

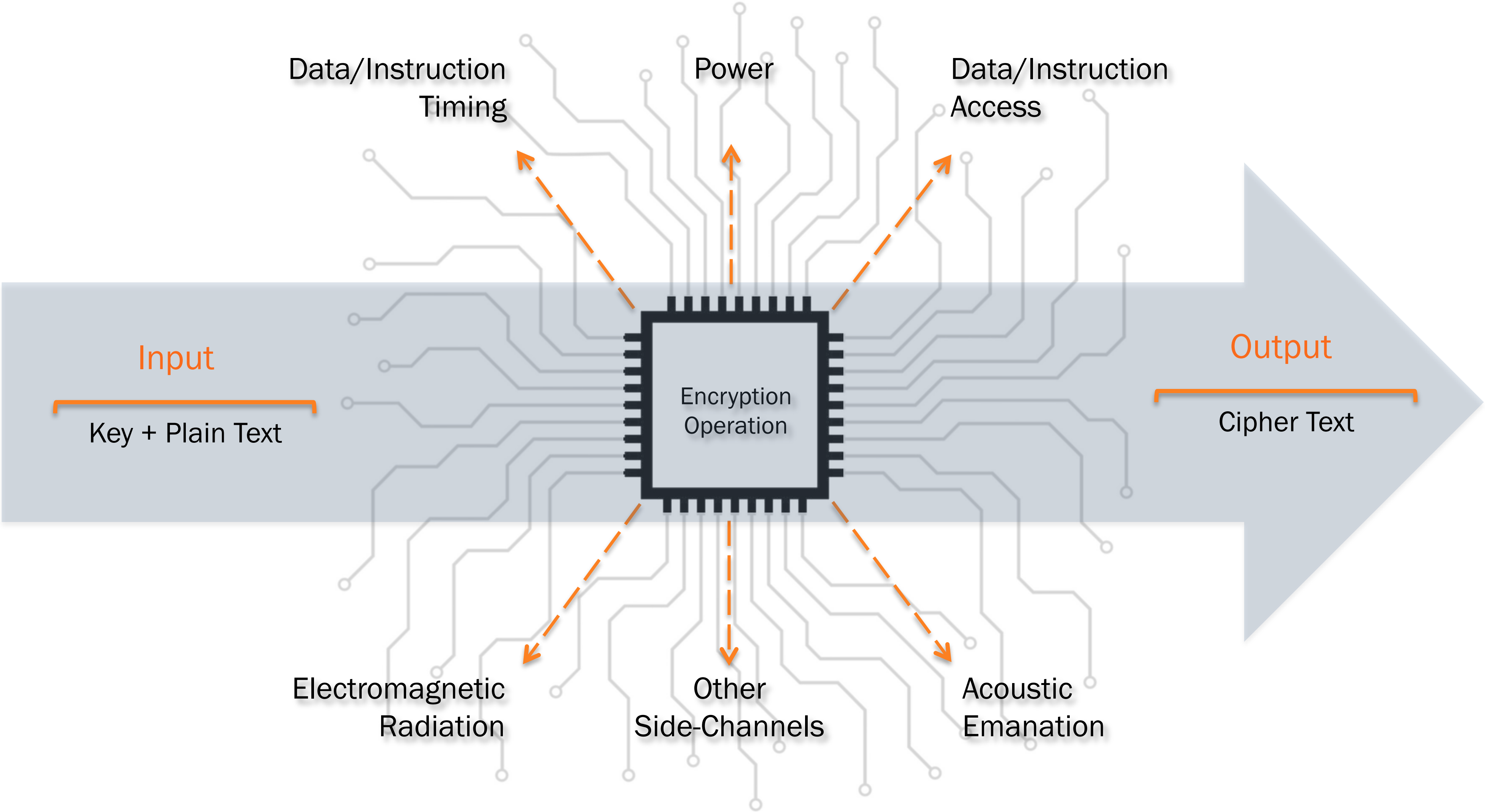
Computing Stack & Privilege Levels

- Information leakage is possible *even under safe* software!
  - Software is often encrypted by mathematically strong encryption techniques [RSA, AES, ECC etc.]
- Underlying hardware is vulnerable
  - Micro-architectural features leak information on the state of program's execution



Information Security

The Side-Channel Leakage



Input

Key + Plain Text

Encryption Operation

Output

Cipher Text

Data/Instruction Timing

Power

Data/Instruction Access

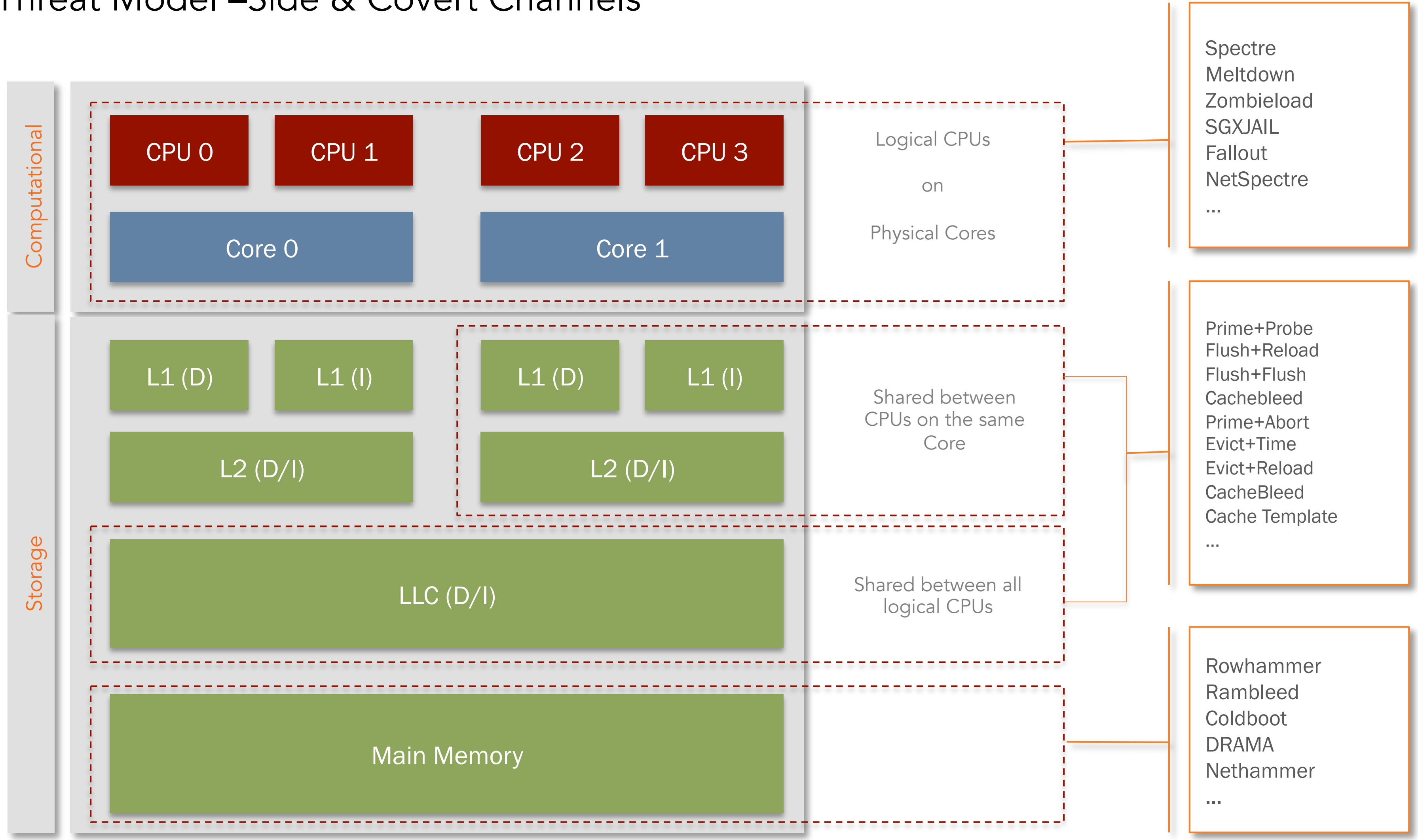
Electromagnetic Radiation

Other Side-Channels

Acoustic Emanation

Information Security

Threat Model –Side & Covert Channels



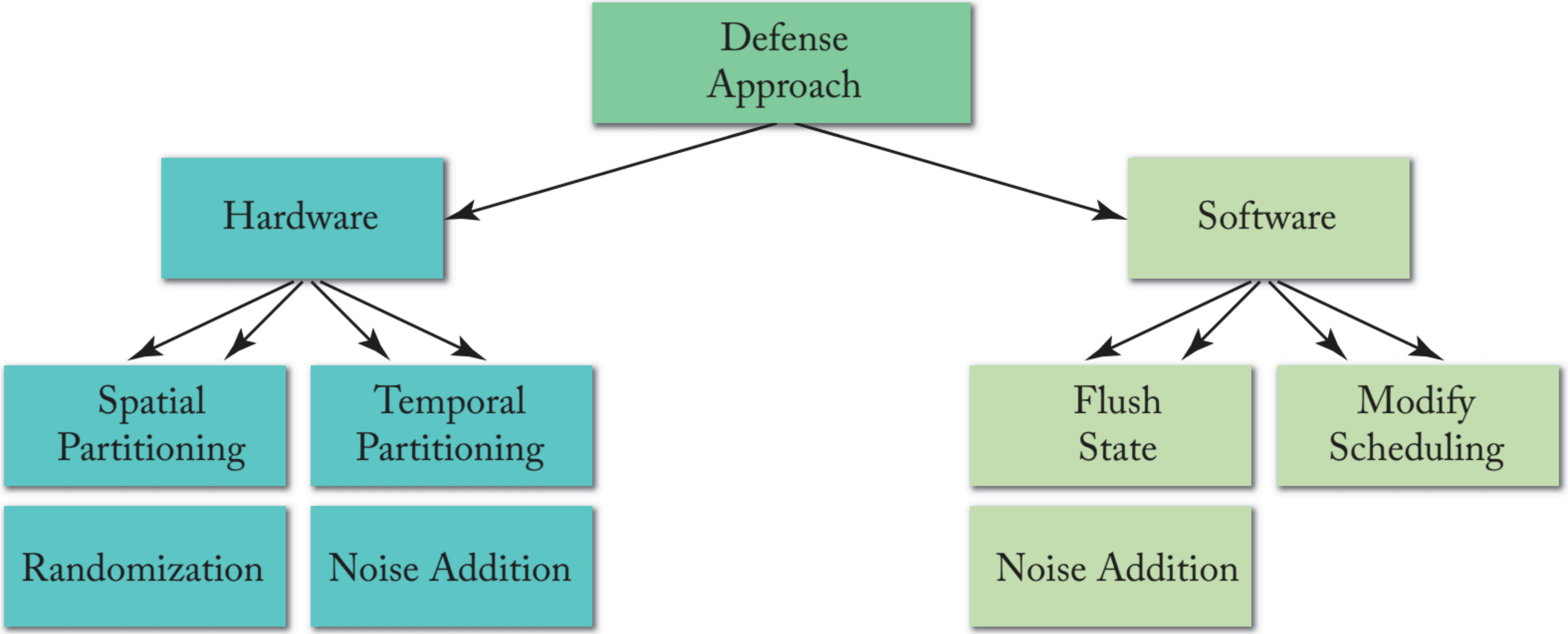
Spectre
Meltdown
Zombieload
SGXJAIL
Fallout
NetSpectre
...

Prime+Probe
Flush+Reload
Flush+Flush
Cachebleed
Prime+Abort
Evict+Time
Evict+Reload
CacheBleed
Cache Template
...

Rowhammer
Rambleed
Coldboot
DRAMA
Nethammer
...

Side & Covert Channels

State-of-the-Art on Defenses



The Way Forward –Conclusive Remarks

① Security has become a first-class design constraint –computing must be seen beyond classics

② Modern security challenges emerge from the *way* we compute today – radical changes at both the hardware & software levels are required

③ No computing platform is secure today and attack surface will expand further–tools are required to contain existing vulnerabilities and future systems must be predictable!

④ Special track on SCADD @ CYBER-2020 offers an opportunity to the academic researchers and industry practitioners to share their work & experiences around the side-channel information leakage issues.

Accepted Papers at SCADD 2020

① Efficient AES Implementation for Better Resource Usage and Performance of IoTs. Umer Farooq, Maria Mushtaq, M. K. Bhatti

② Side Channel Attacks on RISC-V Processors: Current Progress, Challenges, and Opportunities. Mahya Morid Ahmadi, Faiq Khalid, Muhammad Shafique

③ Challenges of Using Performance Counters in Security Against Side-Channel Leakage. Maria Mushtaq, Pascal Benoit, Umer Farooq

④ PCache: Permutation based Cache to Counter Eviction-based Cache-Side Channel Attacks. M. Asim Mukhtar, M. K. Bhatti, Guy Gogniat

⑤ Exploiting Vulnerabilities in Deep Neural Networks: Adversarial and Fault-Injection Attacks. Faiq Khalid, Muhammad Abdullah Hanif, Muhammad Shafique