



Microarchitectural Vulnerabilities - **Assessment and Mitigation**



ICE Seminar

Sep 8, 2022

Maria MUSHTAQ

Avec le soutien de la Fondation Mines-Télécom



About me!

Maria MUSHTAQ, Safe and Secure Hardware (SSH), Communications and Electronics (COMELEC)



Distinctions:

- Portrait of Woman -International face of university @ UBS, France
- Recipient of HiPEAC International Mobility –Yale University, USA
- Recipient of ACM Young Researcher Award –ETH Zurich, Switzerland
- Recipient of Ministry of Defense scholarship
- Recipient of CNRS-Excellent Postdoc grant
- Admissible candidate by the academic jury of CNRS, 2020-2021




Yale University

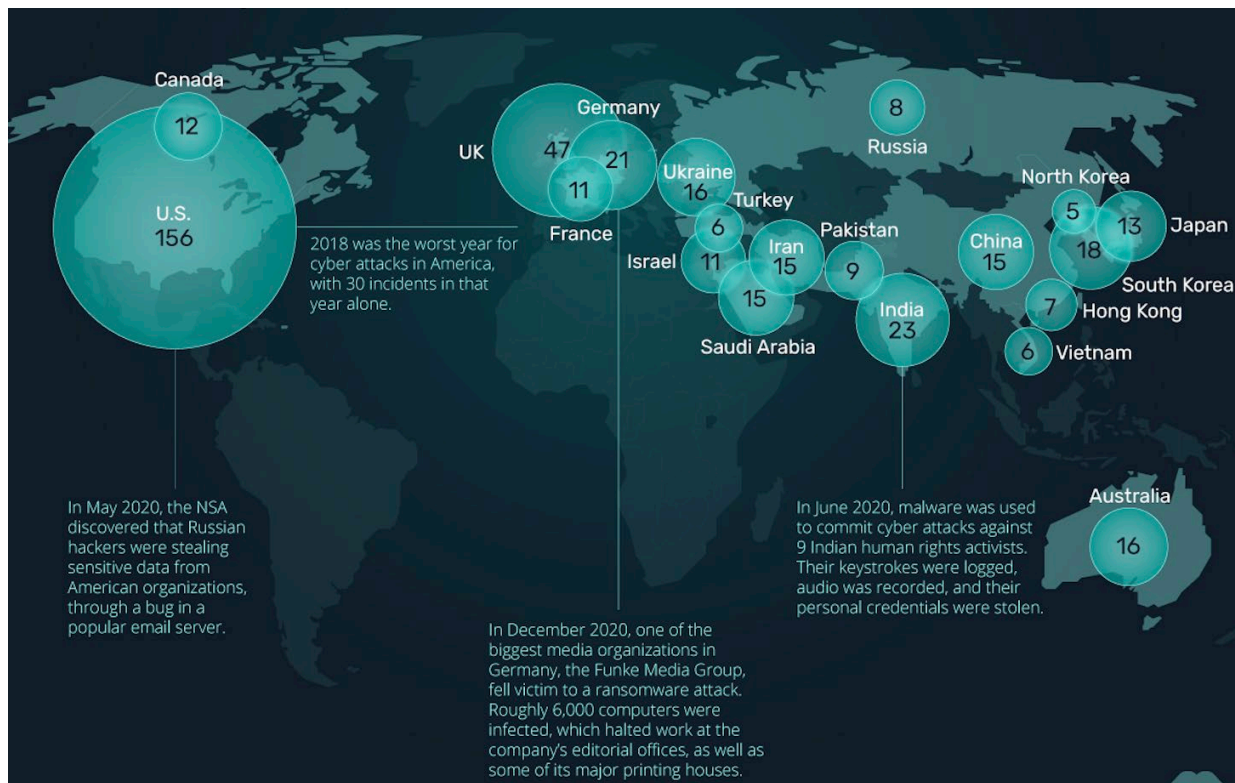
ETH zürich



Outline

- 
- Information Security Perspective
 - Detection Framework
 - Mitigation Framework
 - Conclusions & Future Perspectives

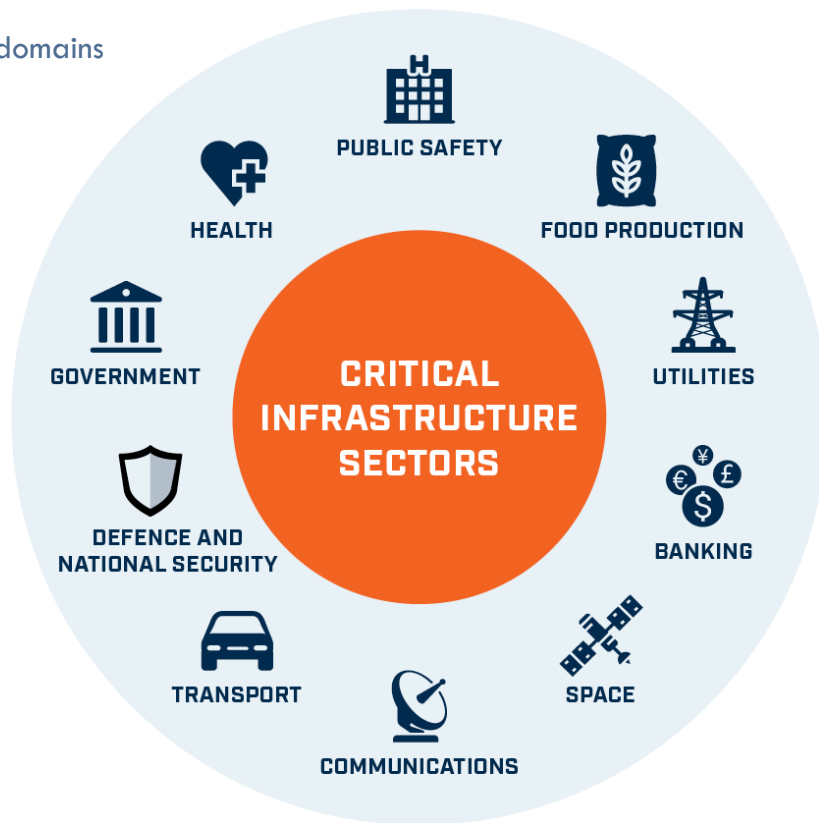
Information Security Perspective



Source: <https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/>

Information Security Perspective

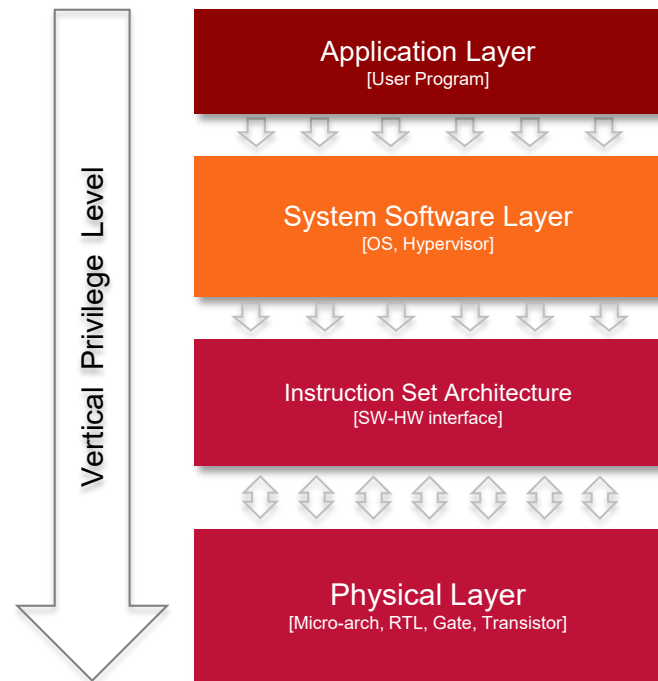
■ A shared concern by many application domains



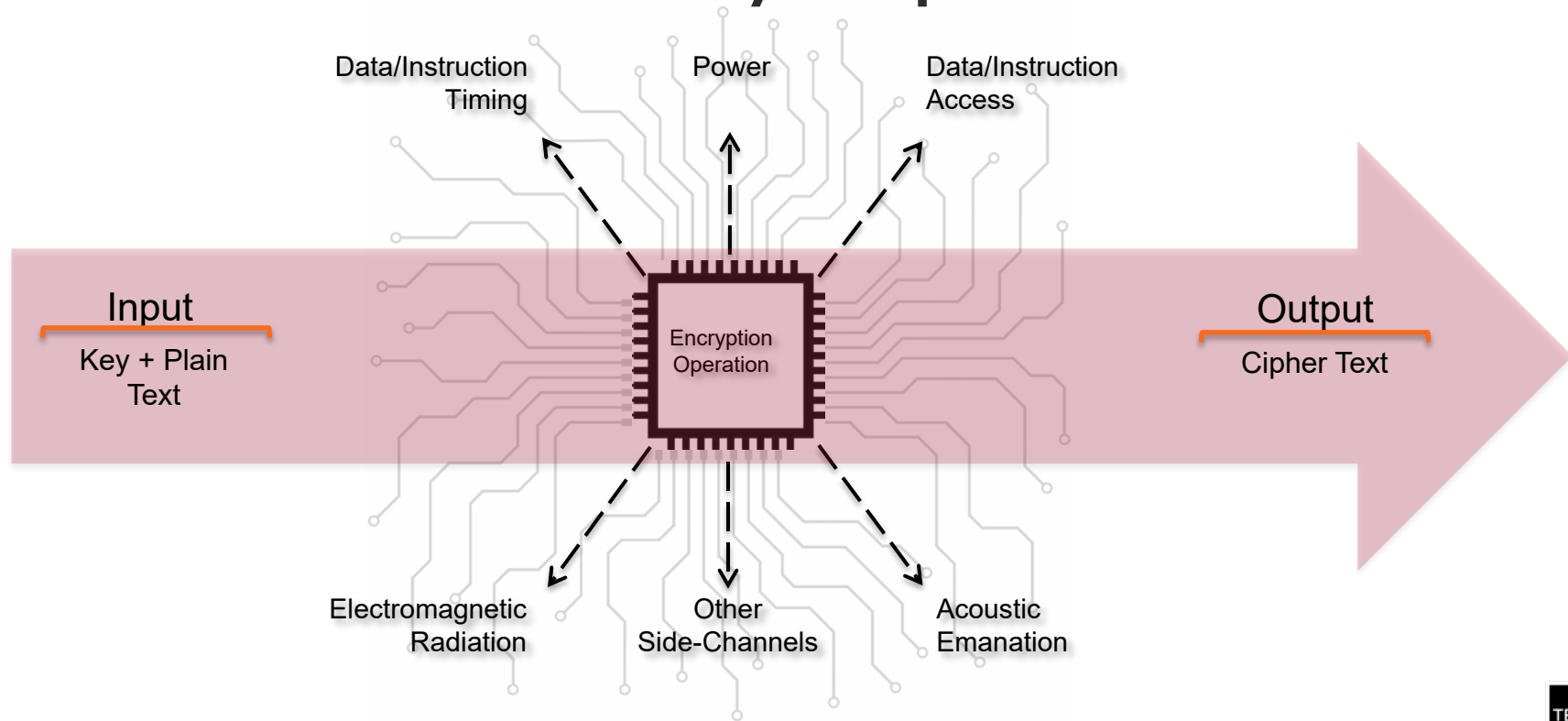
Information Security Perspective

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

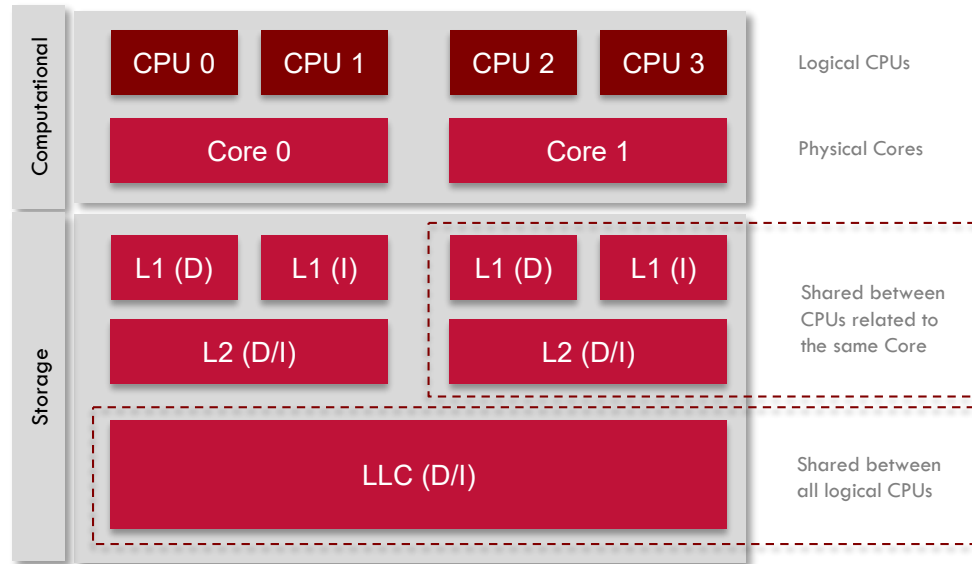


Information Security Perspective



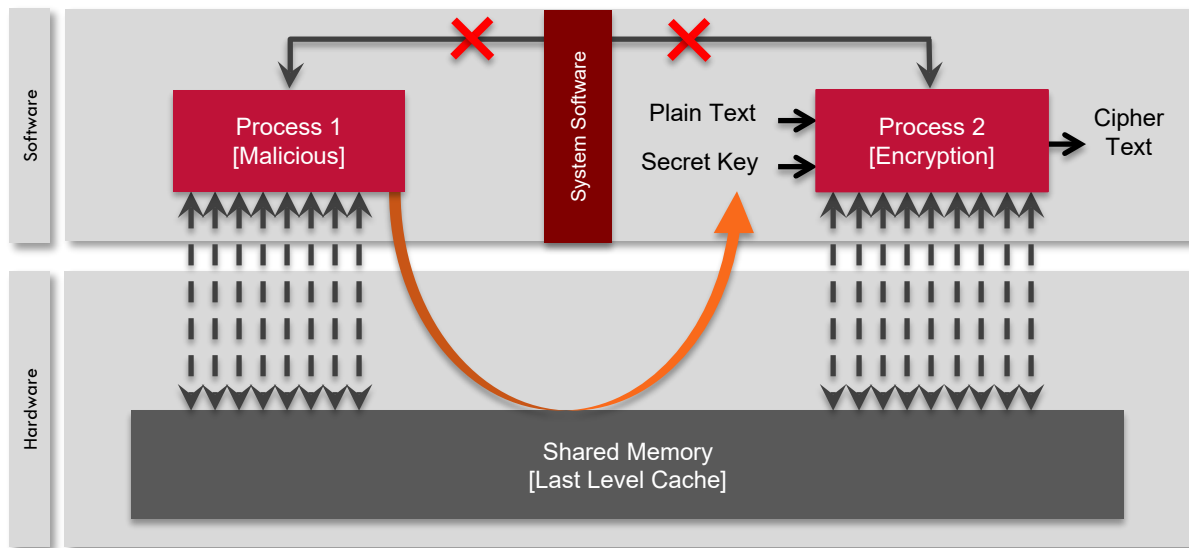
Information Security Perspective

■ Shared Memory Architecture –An Abstract View!



Information Security Perspective

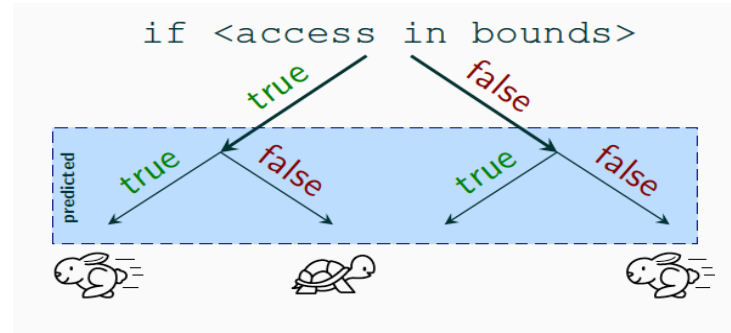
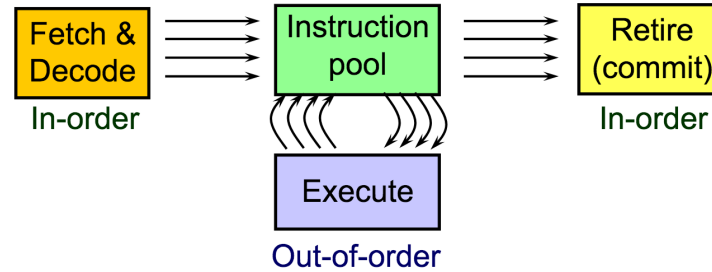
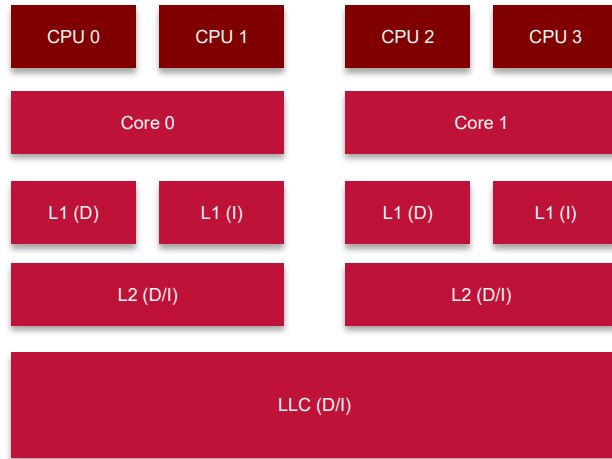
■ Leakage through Shared Memory



Key-dependent memory accesses create timing (Side-Channel) Information!

Information Security Perspective

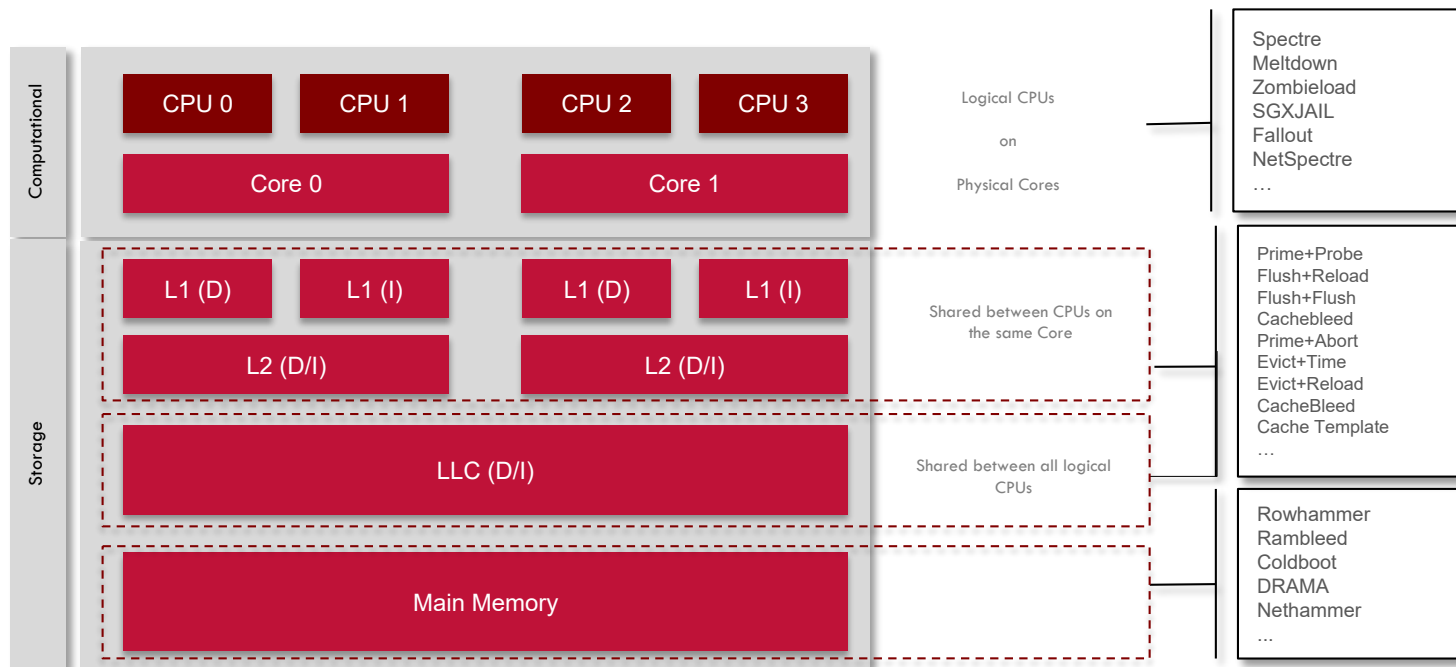
Leakage Through Computational Optimizations



Branch Prediction

Information Security Perspective

■ Intel's x86 –the biggest casualty of security vulnerabilities!



Information Security Perspective

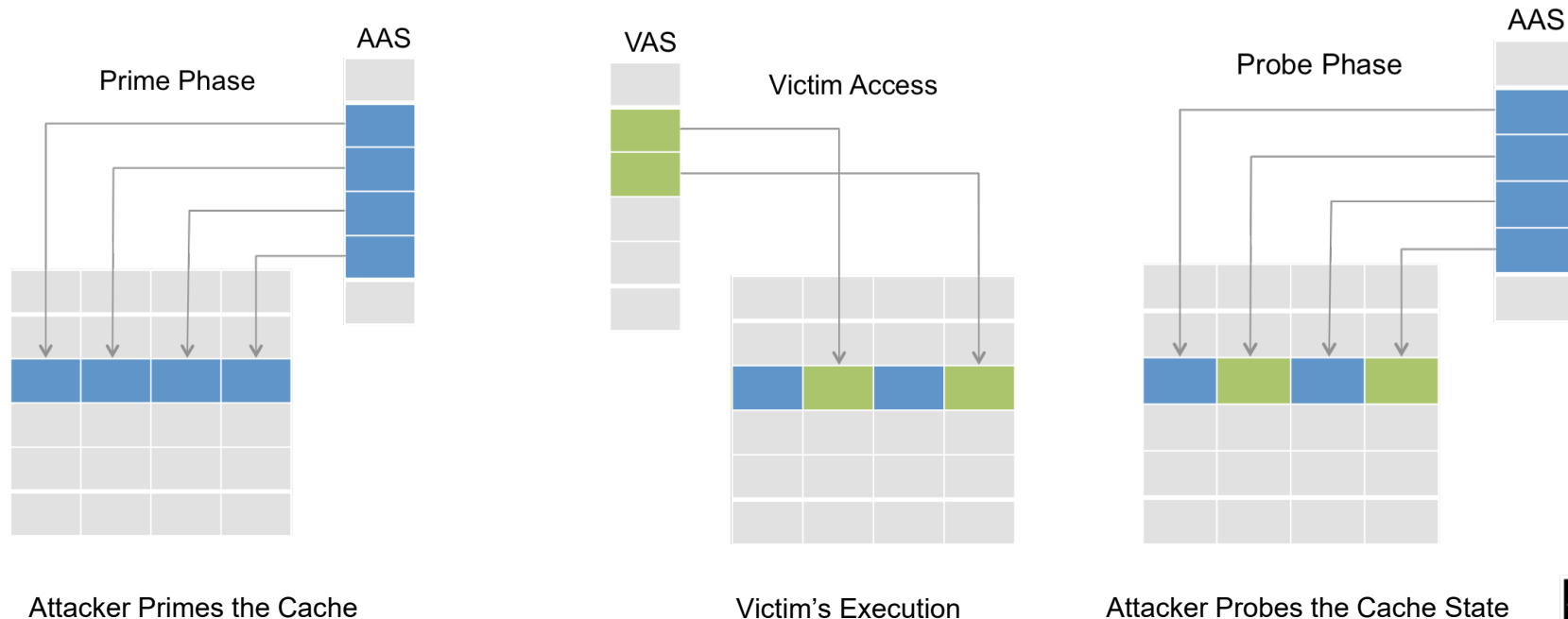
- Threat Model –Why CSCAs are interesting?
 - CSCAs are Non-invasive, Passive & High-resolution
 - CSCAs do not respect privileges
 - They are Cross CPU, Cross Core, Cross VM
 - All CSCAs [and other attacks too] work the same way:
 - Manipulate cache to a known state
 - Wait for the victim to perform its activity
 - Examine what has changed



- Hard to detect as they are part of the hardware design!

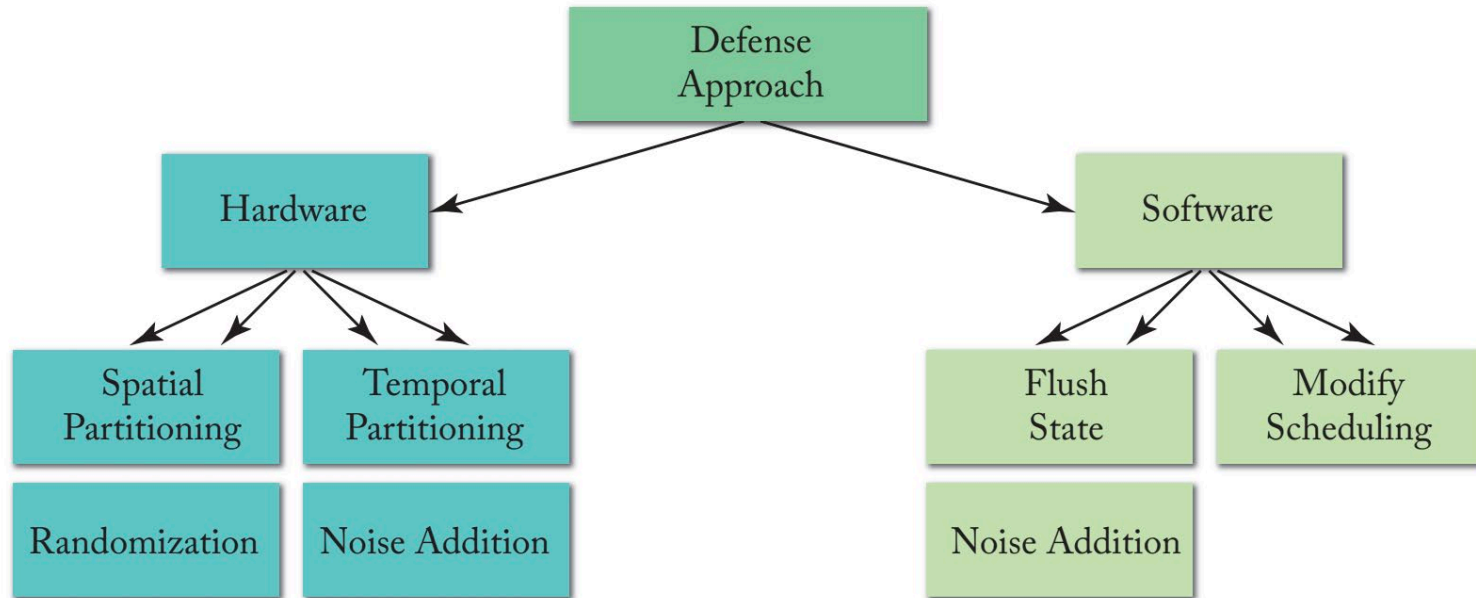
Information Security Perspective

○ Prime+Probe Attack



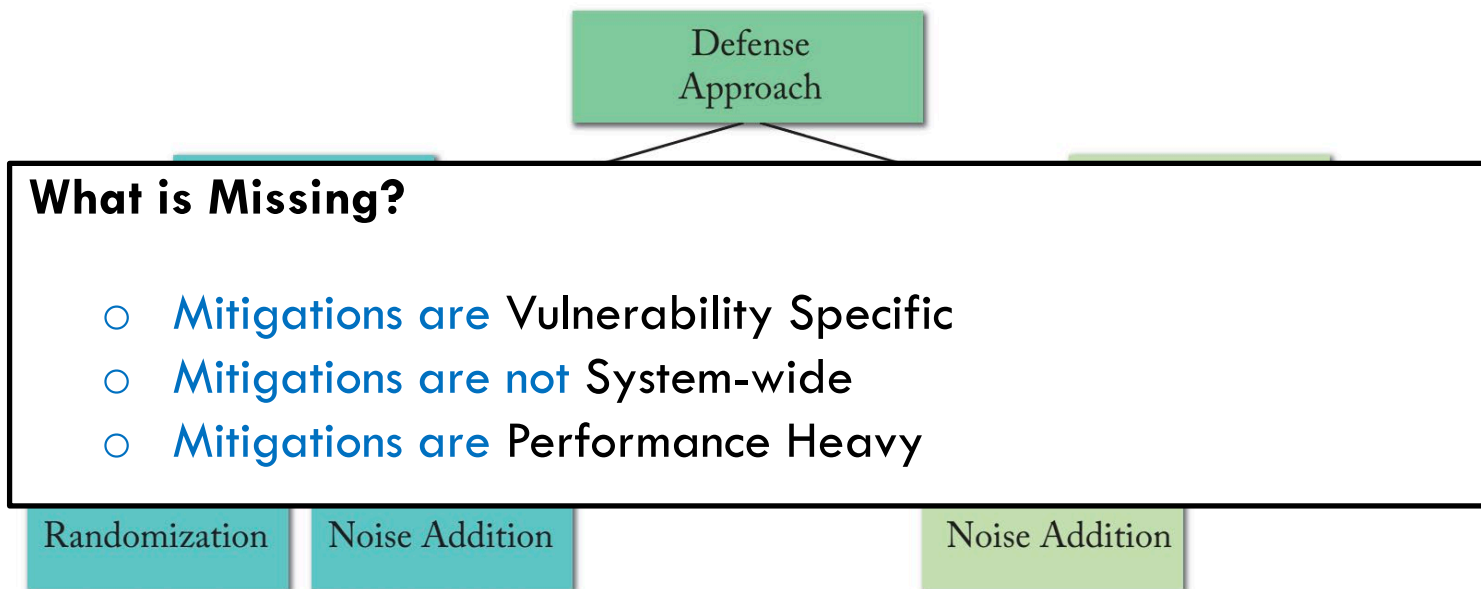
Information Security Perspective

State-of-the-Art on Defenses



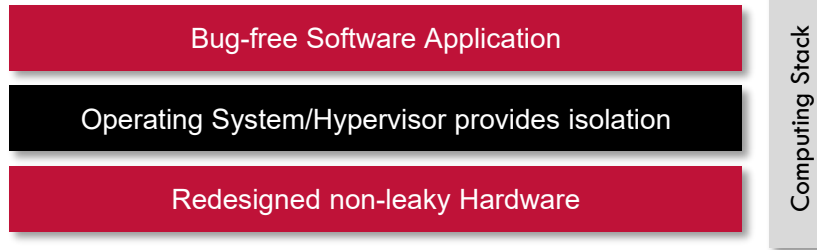
Information Security Perspective

■ State-of-the-Art on Defenses



Information Security Perspective

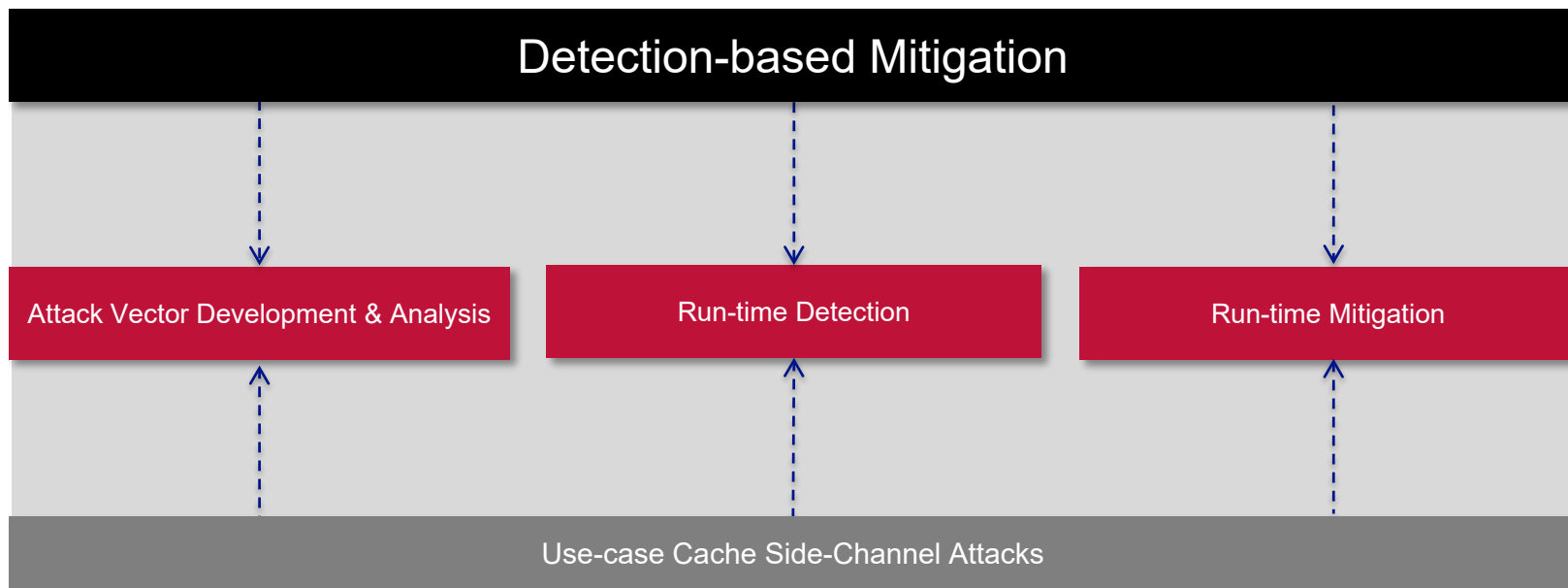
- The Way Forward:
 - Attack surface is not completely known yet –rather expanding!
 - Security paradigm is shifting
- Secure-by-Design –attacks are not feasible in the first place



- Secure at Run-time –attacks can happen, but their impact & value is contained

Research Perspective

■ The Big Picture



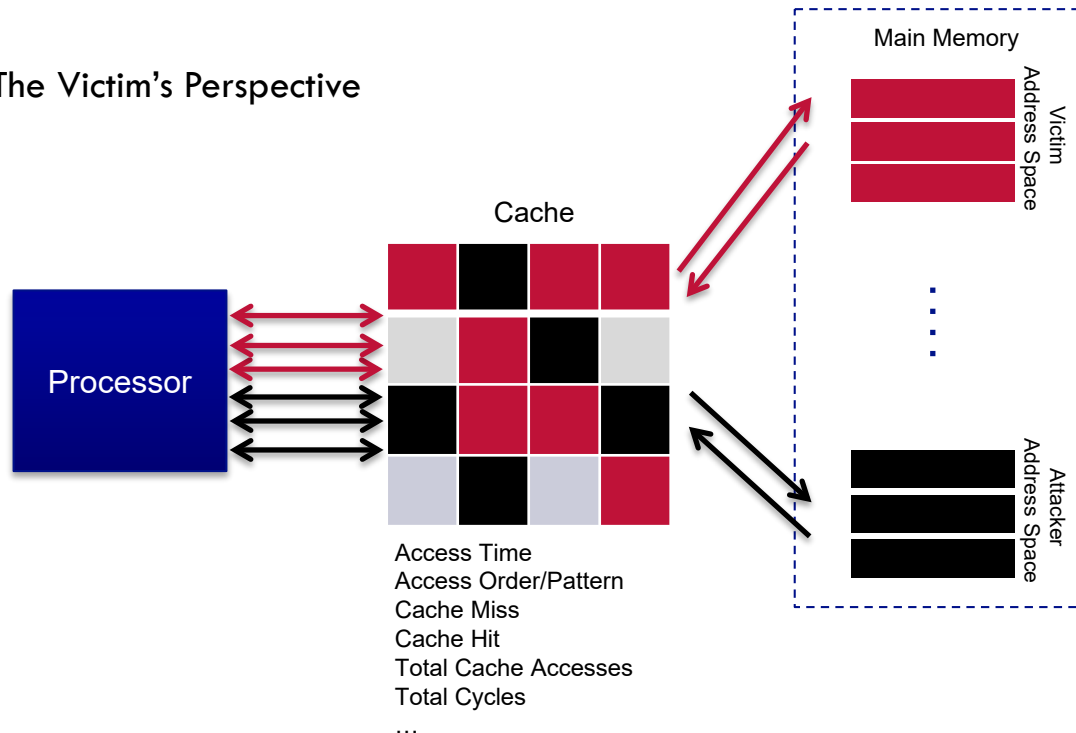
Mukhtar et al., Smart Flush: A Timing Countermeasure against FLUSH+RELOAD Cache-based Side-Channel Attack on RSA. *Published at Elsevier Journal of Systems Architecture* 2020.

Mushtaq et al., Improving Confidentiality Against Cache-based SCAs. *Published at Conference of ACM WomENCourage-2017, Barcelona, Spain.*

Detection Framework

- Cache SCAs affect or alter cache behavior!

- The Victim's Perspective



Detection Framework

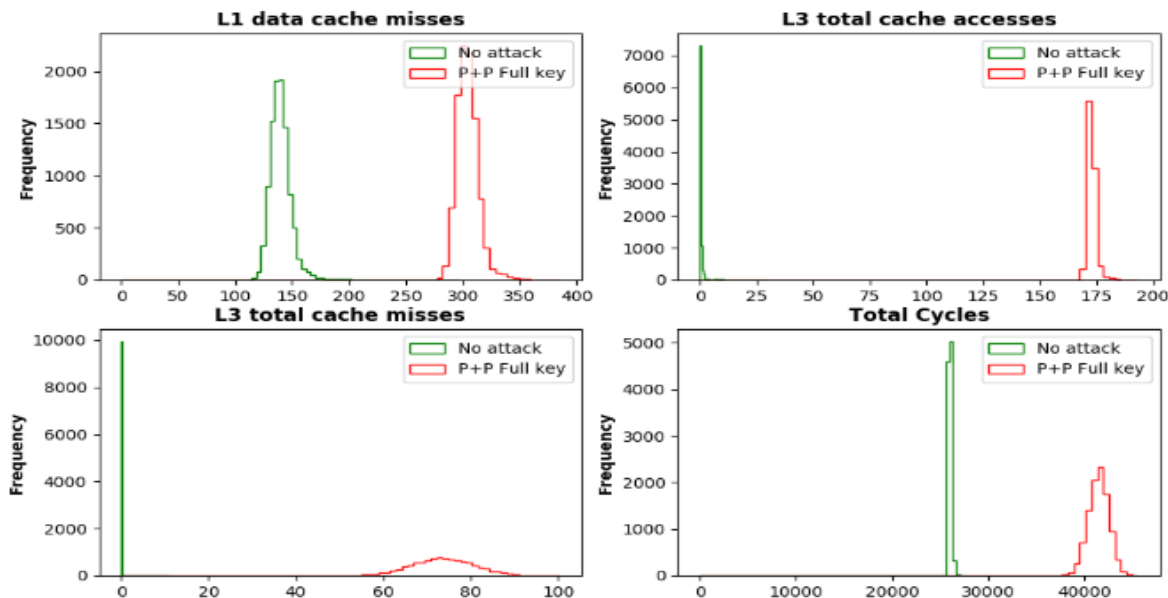
○ Performance Counters as features

#	Scope	Hardware Events
1	Cache Level 1	Data Cache Misses (L1-DCM)
2		Instruction Cache misses (L1-ICM)
3		Total cache misses (L1-TCM)
4	Cache Level 2	Instruction cache accesses (L2-ICA)
5		Instruction Cache misses (L2-ICM)
6		Total Cache accesses (L2-TCA)
7		Total cache misses (L2-TCM)
8	Cache Level 3	Instruction cache accesses (L3-ICA)
9		Total Cache accesses (L3-TCA)
10		Total cache misses (L3-TCM)
11	System-wide	Branch Miss Prediction (BR_MSP)
12		Total CPU Cycles (TOT_CYC)
13		Total Page Faults (Page-Faults)
14		Total Number of Instructions (TOT_INS)
15		Total Branch Instructions (BR_INS)

Mushtaq *et al.*, Challenges of Using Performance Counters in Security Against Side-Channel Leakage, Published at Cyber2020, Nice, France, 2020.

Detection Framework

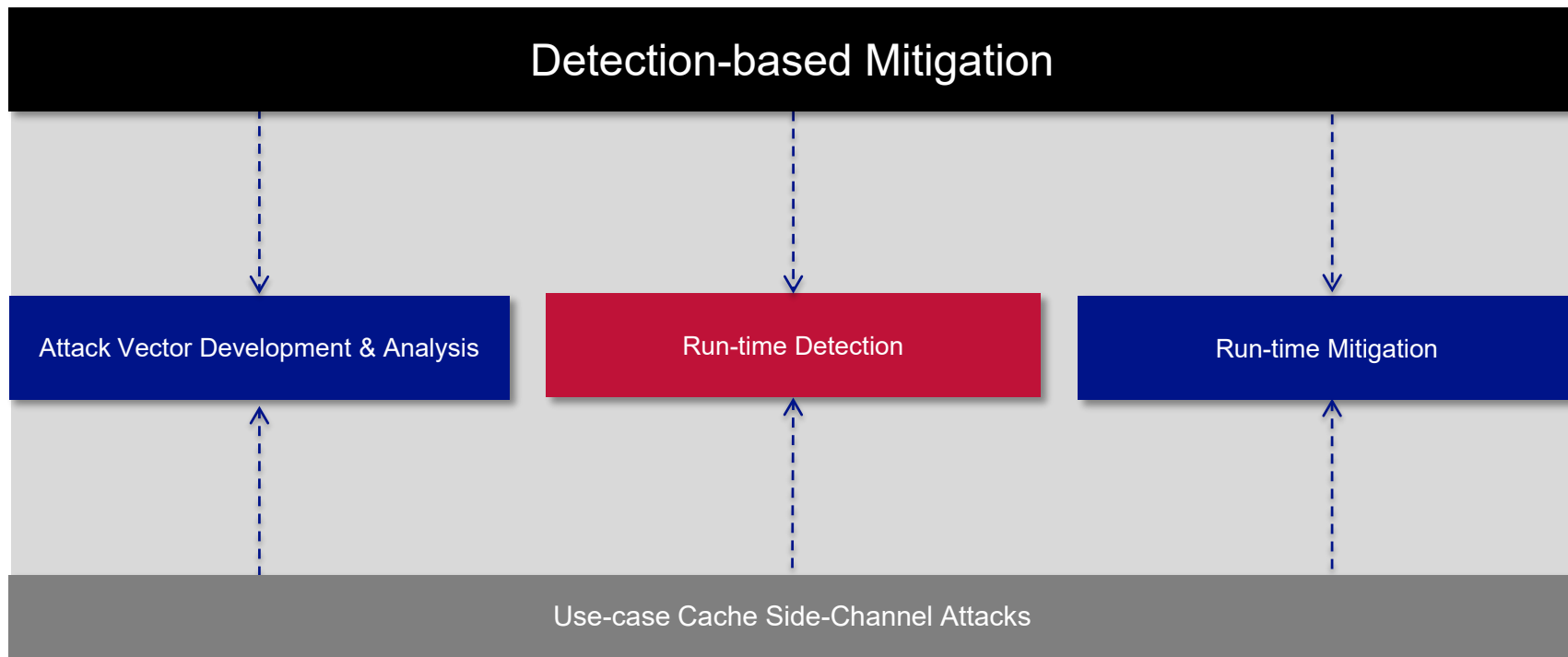
○ Performance Counters –Prime+Probe Attack



Under No Load Conditions

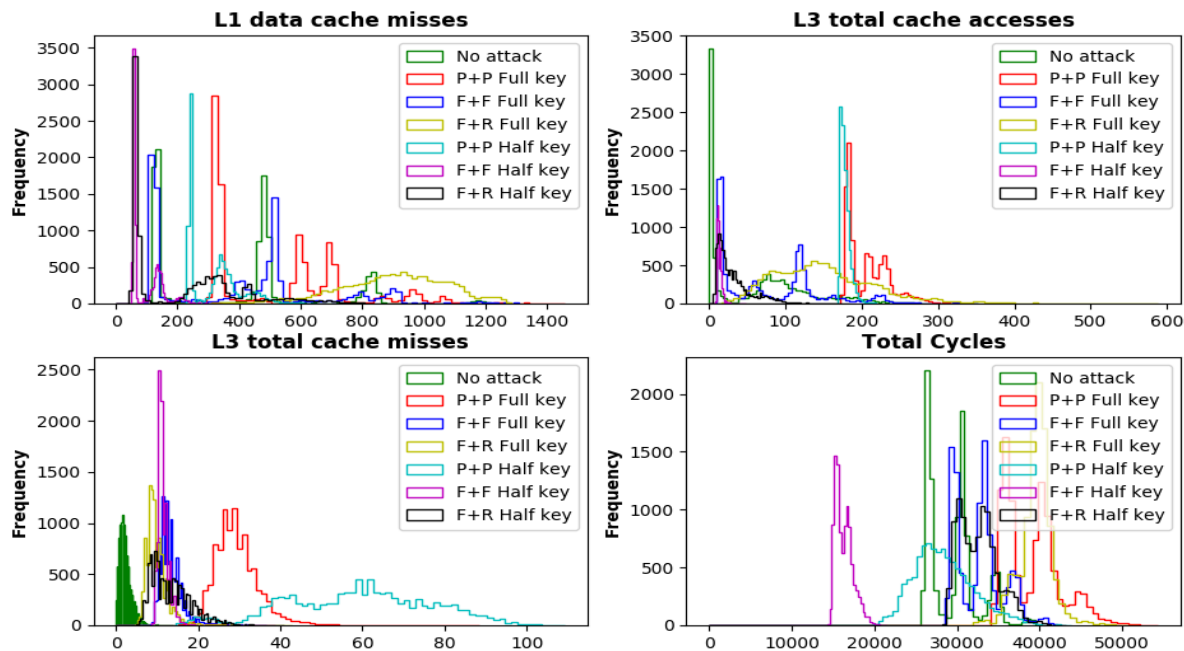
Mushtaq *et al.*, Run-time Detection of Prime+Probe Side-Channel Attack on AES Encryption Algorithm. Published at Global Information Infrastructure and Networking Symposium (GIIS), Thessaloniki, Greece, 2018.

Detection Framework



Detection Framework

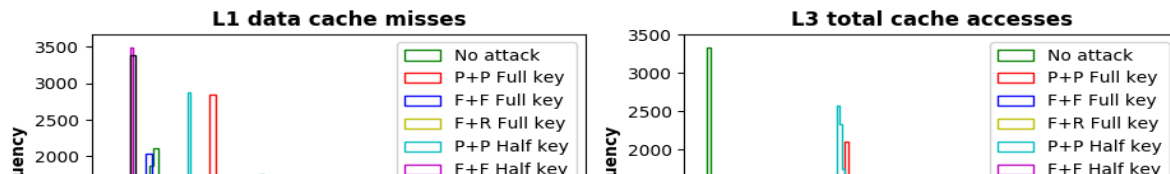
○ Performance Counters



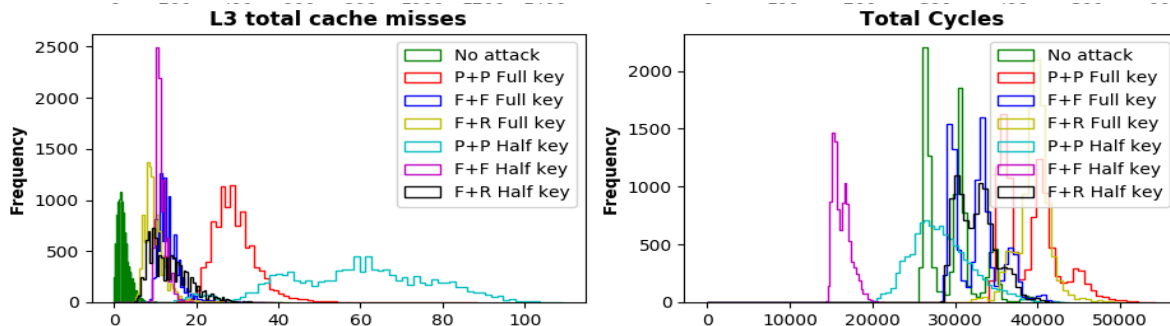
Under Load Conditions
&
Multiple Attacks

Detection Framework

○ Performance Counters



Machine Learning Can Help!



Under Load Conditions
&
Multiple Attacks

Detection Framework

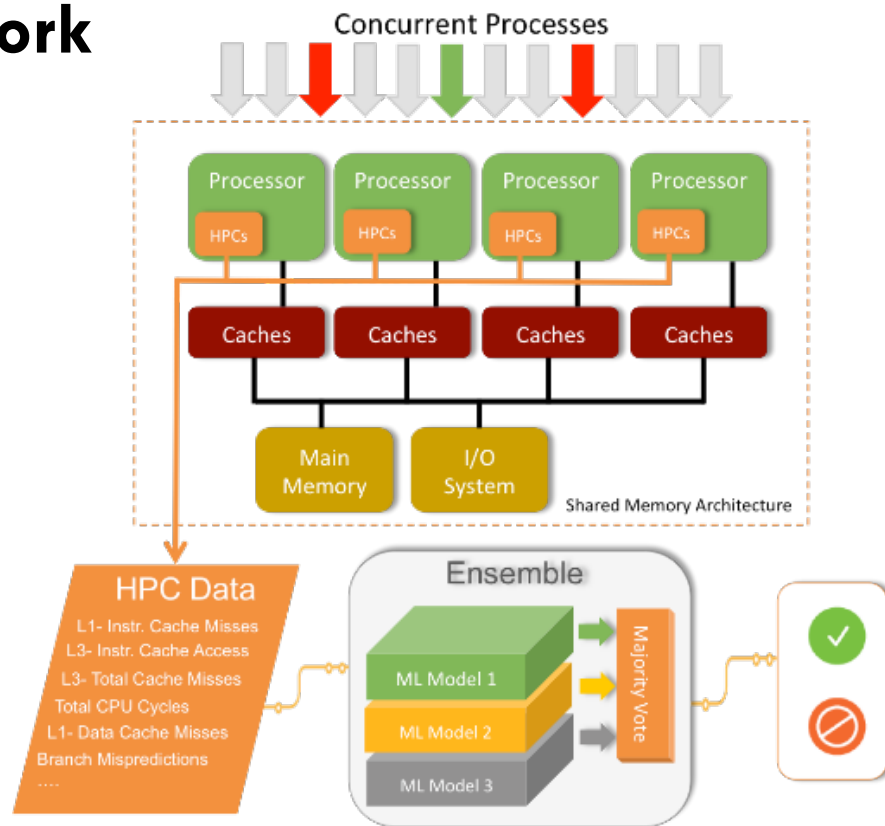
○ Machine Learning Models

#	Machine Learning Model	Type of Model
1	Linear Regression (LR)	Linear
2	Linear Discriminant Analysis (LDA)	Linear
3	Linear Support Vector Machine (SVM)	Linear
4	Quadratic Discriminant Analysis (QDA)	Linear
5	Nearest Centroid	Linear
6	Naïve Bayes	Linear
7	K-Nearest Neighbors (KNN)	Non-Linear
8	Perceptron	Non-Linear
9	Decision Tree	Non-Linear
10	Dummy	Non-Linear
11	Random Forest (RF)	Non-Linear
12	Convolutional Neural Networks (CNNs)	Non-Linear

<https://scikit-learn.org/0.17/modules/classes.html>

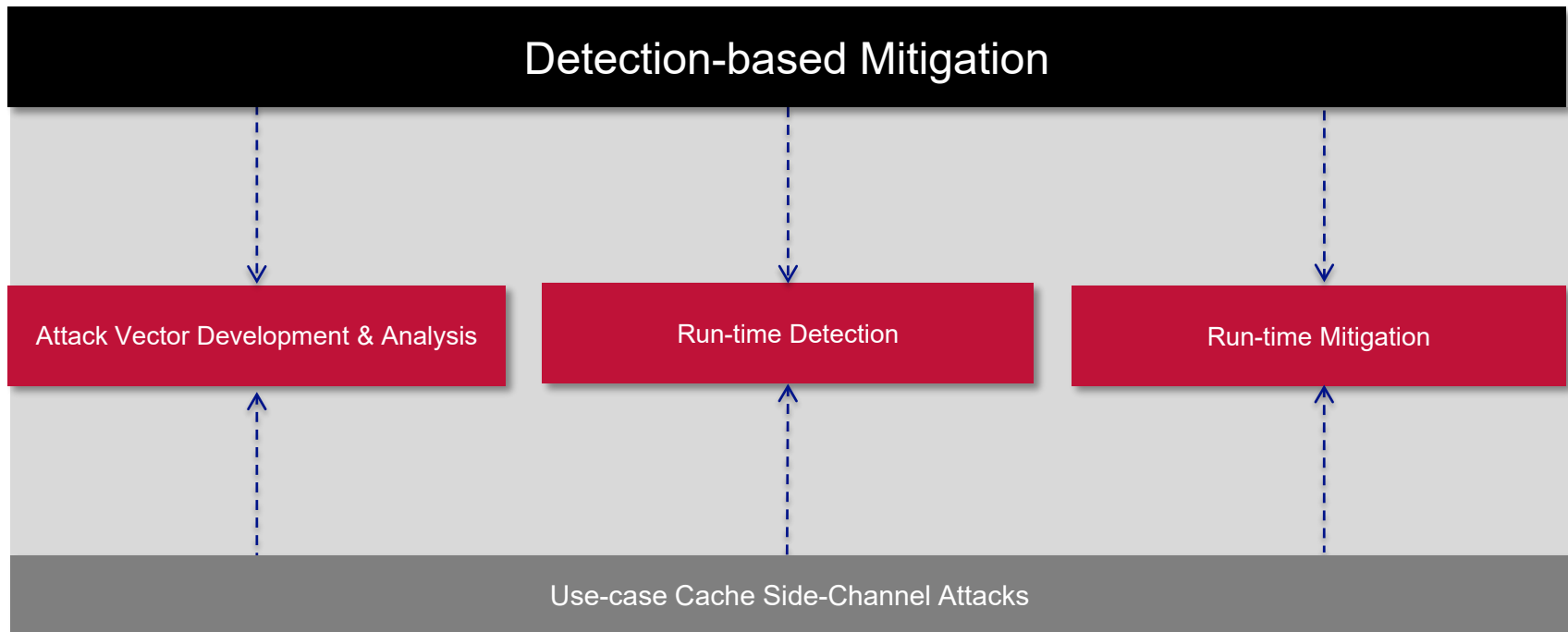
Detection Framework

○ Cache SCA Detection



Detection Framework

■ Proposed Framework –The Big Picture



Detection Framework

■ Use-case Attacks

No.	Use-cases	Cryptosystem	OpenSSL Version	Key Recovery
1	Flush+Reload	RSA	0.9.7l	Full Key
2	Flush+Reload	AES	0.9.7l/ 1.0.1f	Half Key
3	Flush+Reload	AES		Full Key
4	Flush+Flush	AES		Half Key
5	Flush+Flush	AES		Full Key
6	Prime+Probe	AES		Half Key
7	Prime+Probe	AES		Full Key
8	Spectre	Not crypto-specific	Linux Kernel 4.13.037	Full message exploitation
9	Meltdown	Not crypto-specific	Linux Kernel 4.13.037	Full message exploitation

Open source repository of our work:

<https://github.com/ECLab-ITU/Cache-Side-Channel-Attacks>

Detection Framework

F+R Attack on RSA Cryptosystem

Model	Loads	Accuracy (%)	Speed (%)	FP (%)	FN (%)	Overhead (%)
LDA	ZL	99.5	0.9	.498	.002	0.9
	ML	99.5	0.9	0.49	.01	
	HL	99.4	0.9	.527	.073	
LR	ZL	99.5	0.9	0.5	0	1.6
	ML	99.5	0.9	.494	.006	
	HL	99.5	0.9	.462	.038	
SVM	ZL	98.8	0.9	0.4	.78	1.3
	ML	90	0.9	0.17	9.83	
	HL	95.8	0.9	3.21	.99	
QDA	ZL	99.5	0.9	0.5	0	0.6
	ML	99.5	0.9	.494	.006	
	HL	99.4	0.9	0.57	.03	

Mushtaq *et al.*, NIGHTS-WATCH: A Cache-Based Side-Channel Intrusion Detector using Hardware Performance Counters. Published at ISCA-HASP, Los Angeles, CA, USA, 2018.

Mushtaq *et al.*, Sherlock Holmes of Cache Side-Channel Attacks in Intel's x86 Architecture. Accepted at IEEE Conference on Communications and Network Security (CNS), Washington, USA, 2019

Detection Framework

■ Computational Attacks

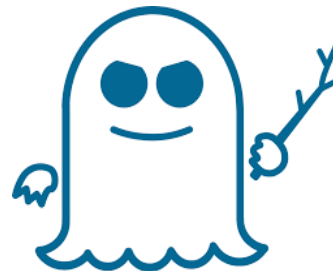
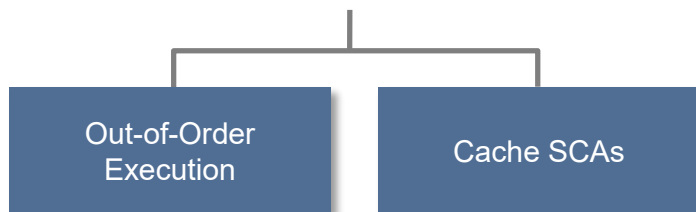


Detection Framework

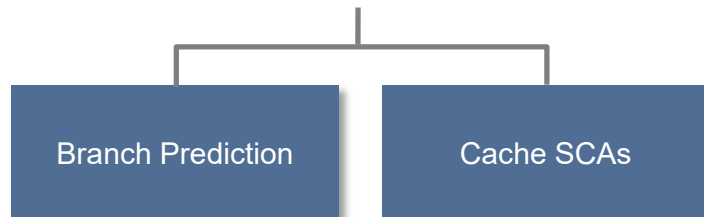
■ Computational Attacks



Meltdown



Spectre



- Two CPU vulnerabilities discovered in 2018!
- Both exploit performance enhancement techniques

Detection Framework



○ Meltdown

- Vulnerability: Permission check for address is done in parallel & out-of-order to the load instruction!

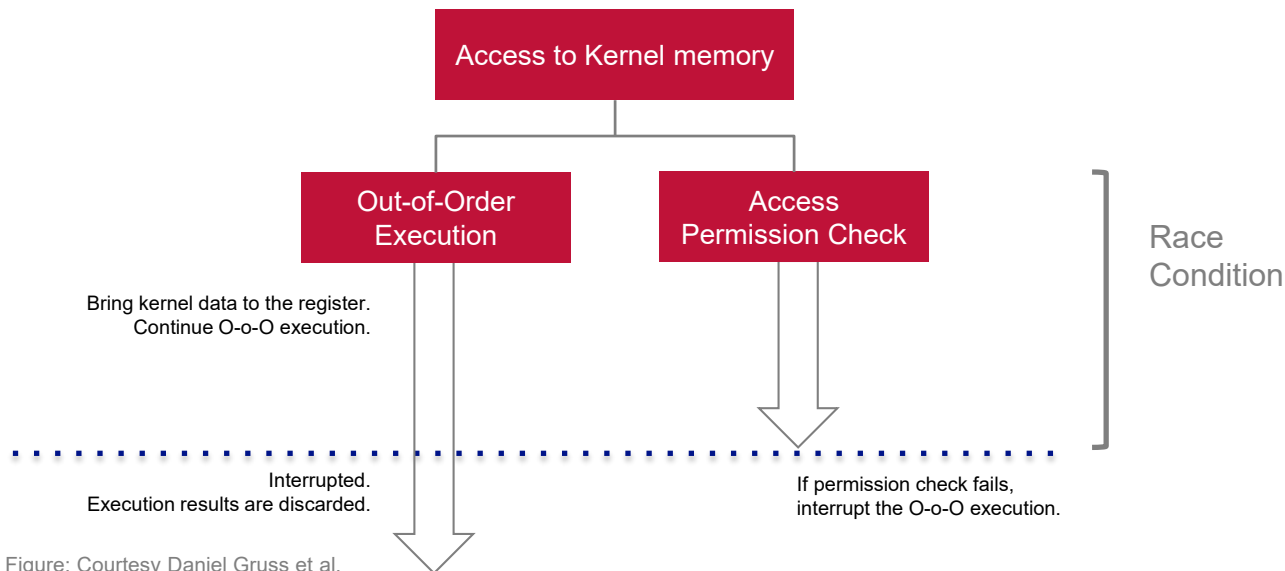


Figure: Courtesy Daniel Gruss et al.

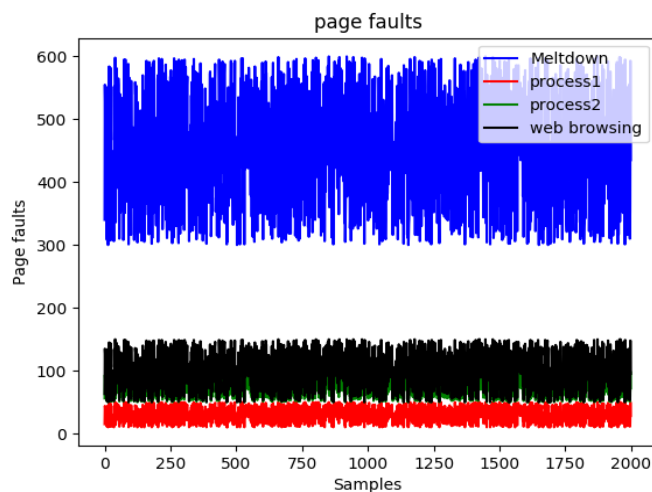
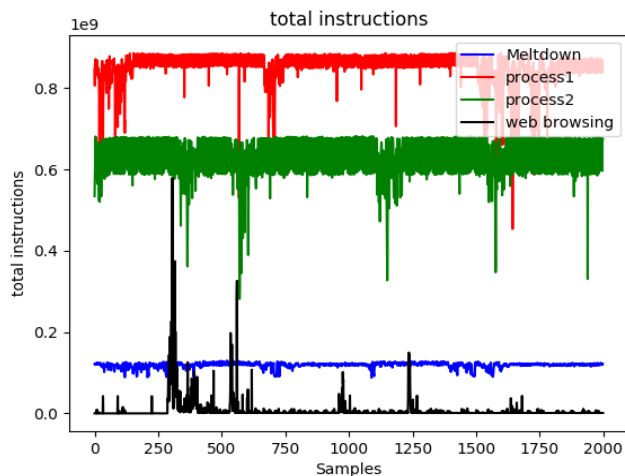
Detection Framework



○ Meltdown Detection

○ Selected HPCs & SPCs

Scope of event	Hardware event	Feature ID
L3 cache	Total cache misses	L3_TCM
L3 cache	Total cache accesses	L3_TCA
System wide	Total page faults	page_faults
System wide	Total number of instructions	TOT_INS



Detection Framework



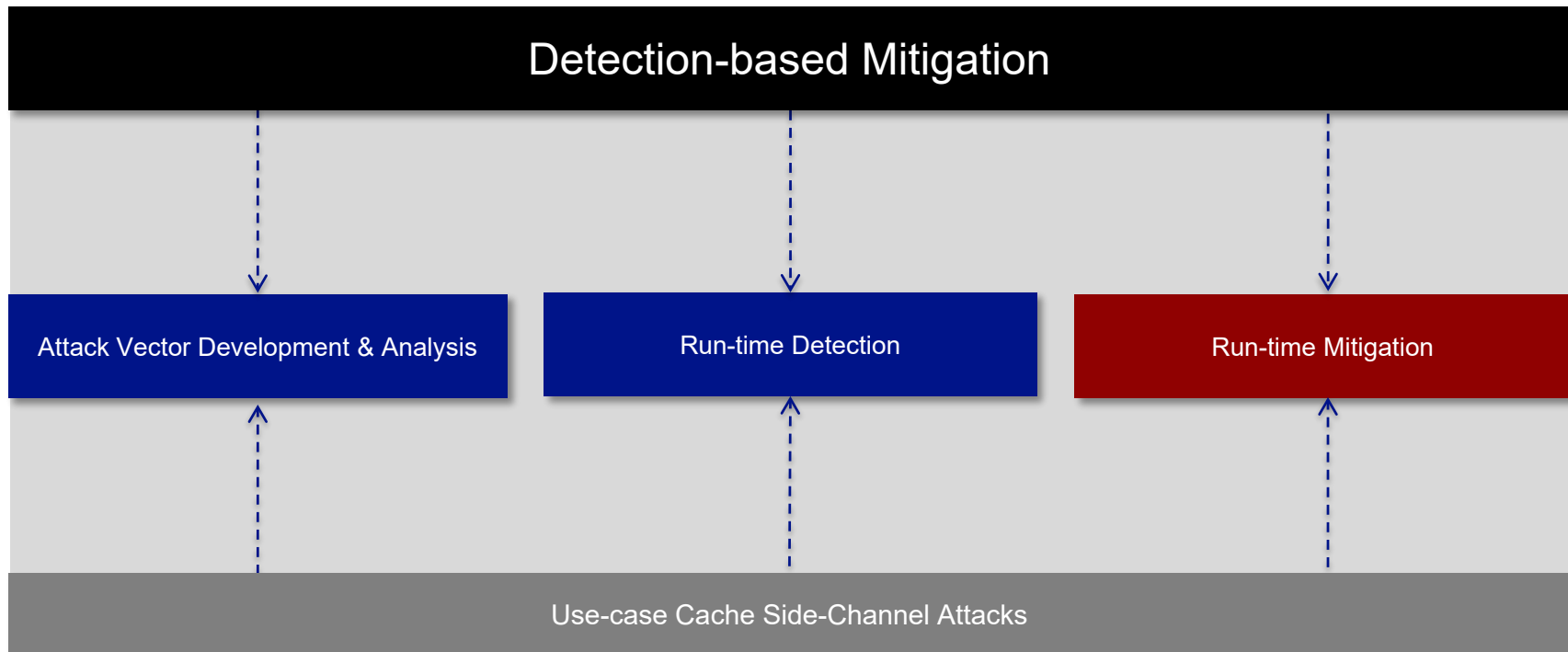
○ Meltdown Detection

Model	Load	Accuracy (%)	Speed (μ s)	FP (%)	FN(%)	Overhead (%)
LDA	NL	99.99	10	0.01	0	1.91
	AL	99.91	10	0.09	0	
	FL	98.30	10	1.25	0.45	
LR	NL	99.41	10	0.59	0	2.21
	AL	97.45	10	1.95	0.60	
	FL	96.00	10	3.40	1.60	
SVM	NL	99.99	10	0.01	0	2.00
	AL	99.40	10	0.60	0	
	FL	98.35	10	1.39	0.26	

Mushtaq *et al.*, Transit-Guard: An OS-based Defense Mechanism Against Transient Execution Attacks, Published at IEEE European Test Symposium, 2021.

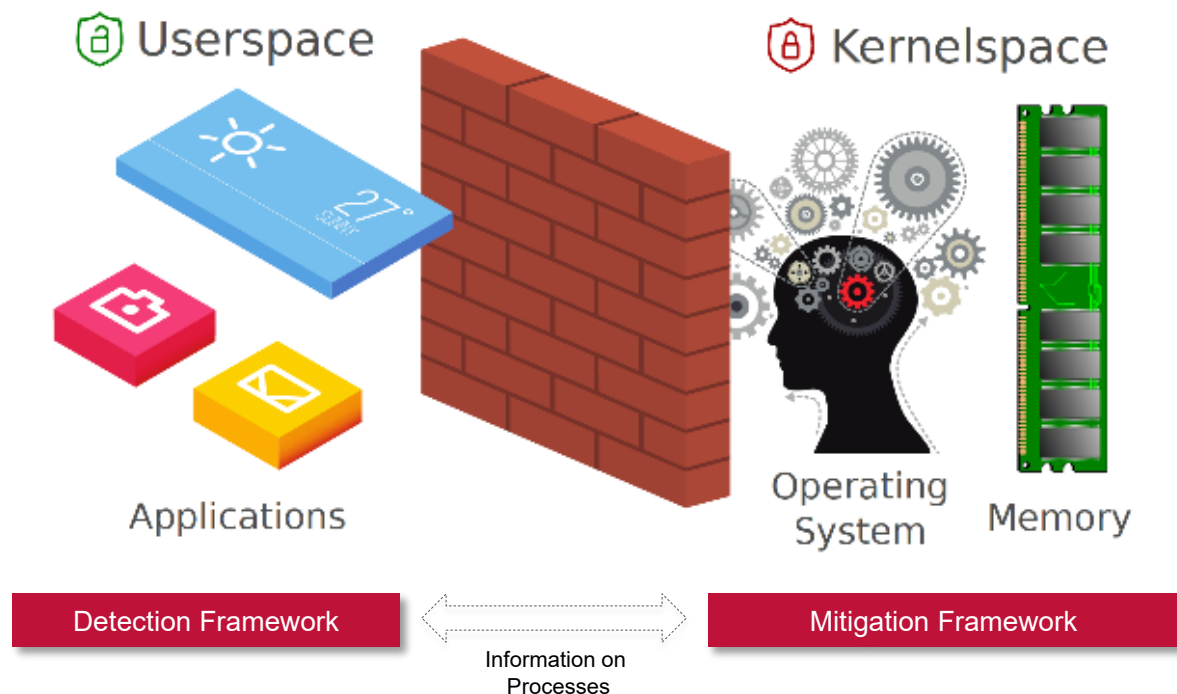
Mitigation Framework

■ Proposed Framework –The Big Picture



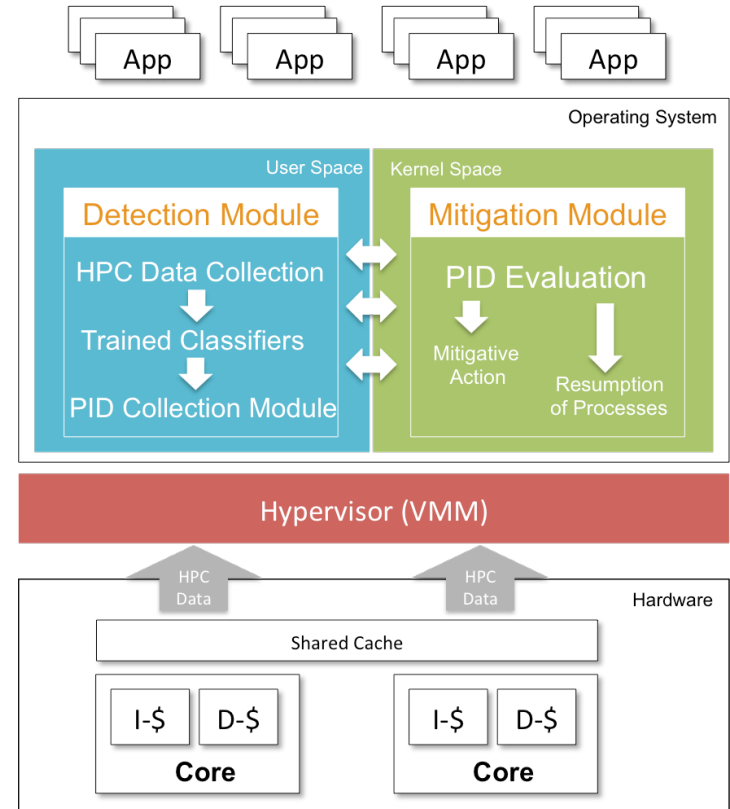
Mitigation Framework

- Simultaneous Attacks, Detection and Mitigation



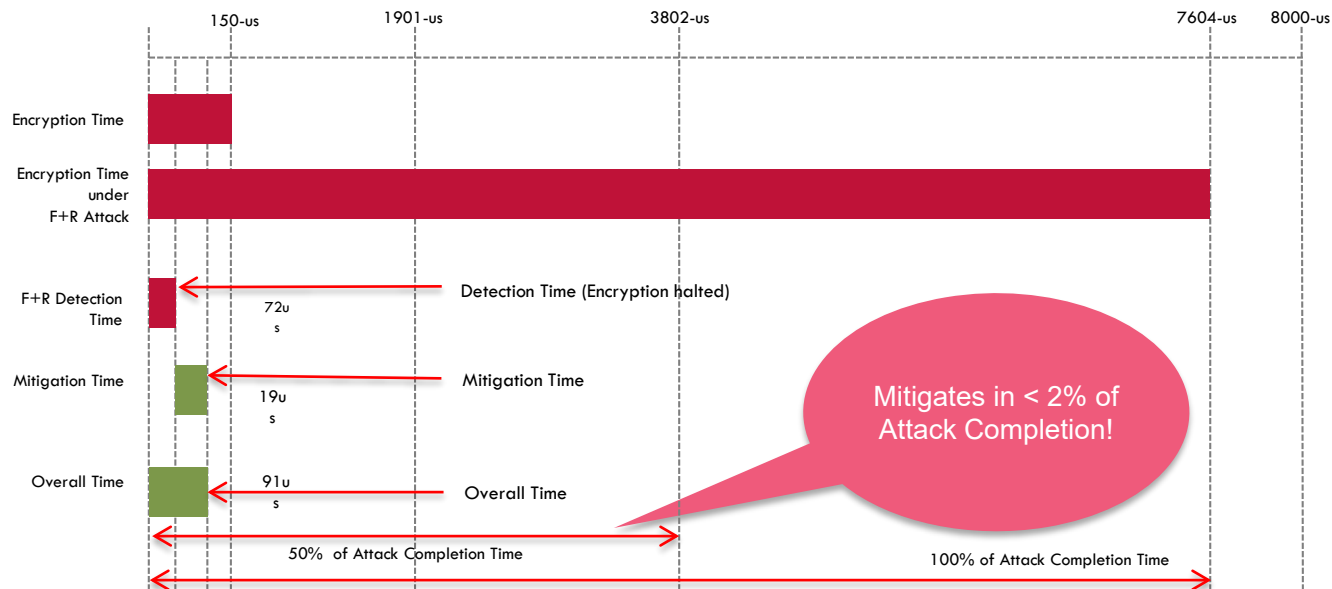
Mitigation Framework

- Detection-based Protection under Linux




Mitigation Framework

Detection-based Mitigation of F+R Attack on RSA



Mushtaq et al., The Kingsguard: OS-level mitigation against cache-channel attacks using run-time detection, Published at IEEE-Access, 2022.

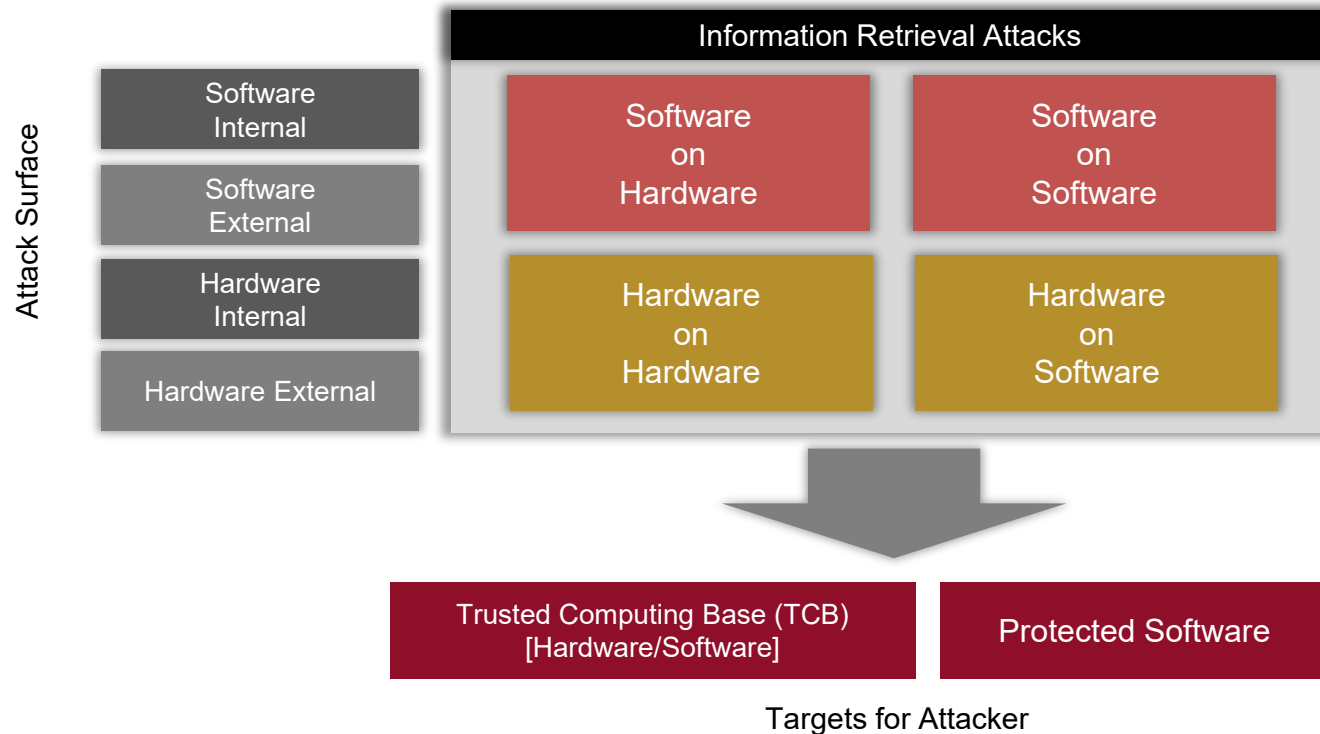
Outline

- 
- Information Security Perspective
 - Detection Framework
 - Mitigation Framework
 - Conclusions & Future Perspectives

Conclusions –at large

- Side channel information leakage is powerful & attack surface is expanding
- Need-based protection has the potential to contain SCAs, both computational & storage, while retaining the performance benefits
- Detection is promising –can serve as the first line of defense in the absence of secure-by-design solutions
- Machine learning can help improving security –use of specialized ML models and deep learning

Future Perspectives

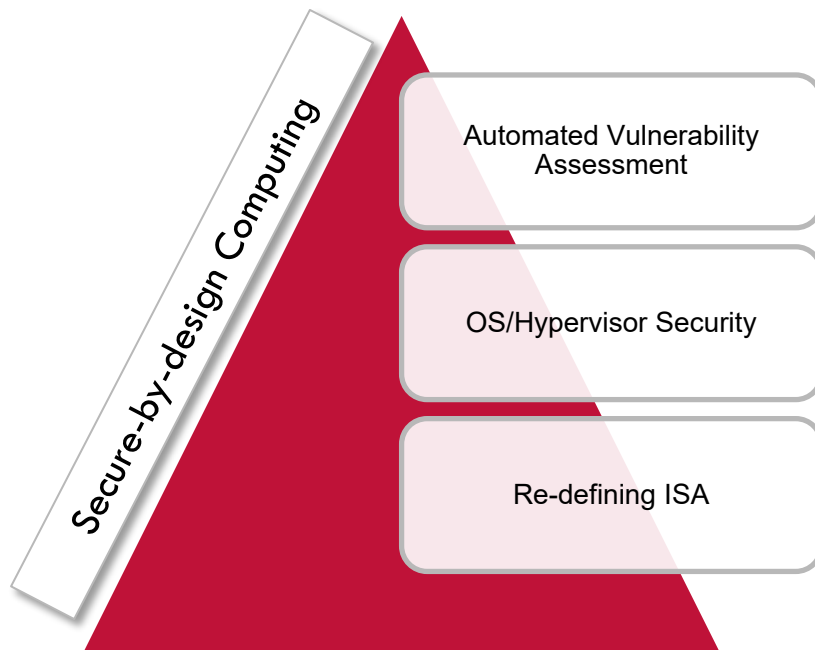


Future Perspectives

- Security has become a 1st class design constraint –computing must be seen beyond classics
- Modern security challenges emerge from the way we compute today –radical changes at both the hardware & software levels are required
- 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!

Research Activities

**WE'RE
HIRING!**



Awareness Seminar

IP Paris & Telecom's 1st International Winter School on Microarchitectural Security – 5-9th of December 2022

[ABOUT](#)[EDUCATION](#)[RESEARCH](#)[INNOVATION](#)[CAMPUS](#)

[HOME](#) – INTERNATIONAL WINTER SCHOOL ON MICROARCHITECTURAL SECURITY 2022

About

SHARE



International Winter School on Microarchitectural Security 2022

The International Winter School on Microarchitectural Security (Mic-Sec) offers academic and industrial talks along with hands-on experience on attacks, software and hardware countermeasure techniques with a special focus on side-channel attacks. The Mic-Sec Winter School 2022 edition will take place at the FIAP Paris from the 5th to the 9th of December 2022 in Paris, France.

<https://www.ip-paris.fr/en/international-winter-school-microarchitectural-security-2022>

<https://www.ip-paris.fr/en/news/winter-school-microarchitectural-security-complex-and-transdisciplinary-emerging-subject>

<https://imtech.imt.fr/en/2022/09/07/side-channel-attacks-how-to-exploit-vulnerabilities-of-processors/>



Thank You!

[Discussion]



Maria.Mushtaq@telecom-paris.fr



@Maria_Mushtaq_