System Security Group

Can’t see the Forest for All the TEEs

Moritz Schneider
Zero Trust Hardware Architectures
Workshop

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)
- Trusted Computing

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)
- Trusted Computing
- Trustlets (ARM)

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)
- Trusted Computing
- Trustlets (ARM)
- Zero trust

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)
- Trusted Computing
- Trustlets (ARM)
- Zero trust
- Enclave (Intel)

Naming Jungle

- Confidential Computing (NVIDIA, Amazon, Microsoft)
- Trusted Computing
- Trustlets (ARM)
- Zero trust
- Enclave (Intel)
- Secure VM (AMD, IBM)

Trusted Execution Environment

Definition?

Definition?

CONFIDENTIAL COMPUTING CONSORTIUM

Definition?

CONFIDENTIAL COMPUTING CONSORTIUM

TRUSTED® COMPUTING GROUP

Definition?

CONFIDENTIAL COMPUTING CONSORTIUM

TRUSTED® COMPUTING GROUP

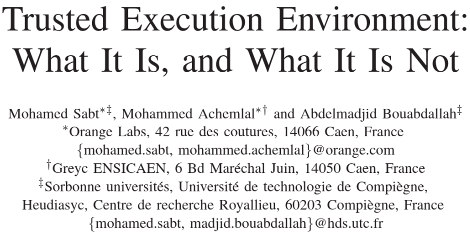
GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Definition?

CONFIDENTIAL COMPUTING CONSORTIUM

TRUSTED® COMPUTING GROUP

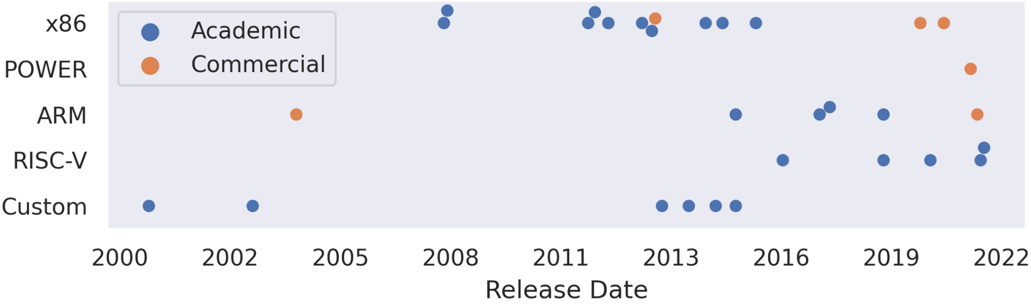
GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES



Trusted Execution Environment: What It Is, and What It Is Not

Mohamed Sabt[*‡], Mohammed Achemlal[*†] and Abdelmadjid Bouabdallah[‡]
[*]Orange Labs, 42 rue des coutures, 14066 Caen, France
{mohamed.sabt, mohammed.achemlal}@orange.com
[†]Greyc ENSICAEN, 6 Bd Maréchal Juin, 14050 Caen, France
[‡]Sorbonne universités, Université de technologie de Compiègne,
Heudiasyc, Centre de recherche Royallieu, 60203 Compiègne, France
{mohamed.sabt, madjid.bouabdallah}@hds.utc.fr

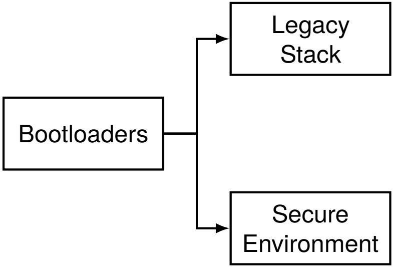
TEEs

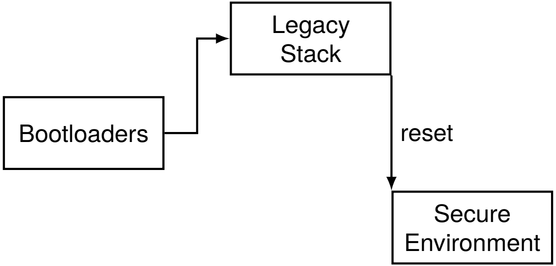

x86
POWER
ARM
RISC-V
Custom
● Academic
● Commercial
2000
2002
2005
2008
2011
2013
2016
2019
2022
Release Date

The Features of TEEs

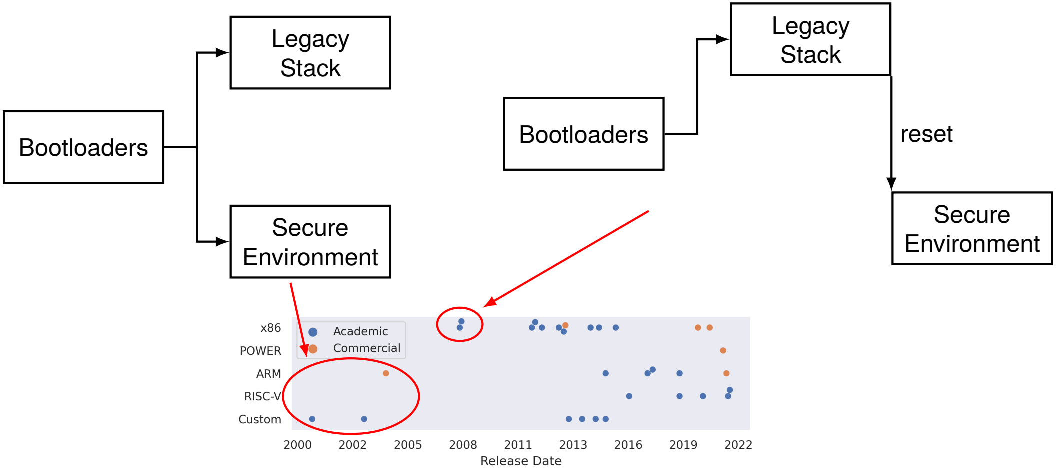
- Verifiable Launch
- Runtime Isolation
- Cryptographic Memory Protection
- Secure Storage
- Trusted IO
- Physical Adversary?
- Migration
- etc.

Verifiable Launch: Static vs Dynamic Boot





Verifiable Launch: Static vs Dynamic Boot



Bootloaders

Legacy Stack

Secure Environment

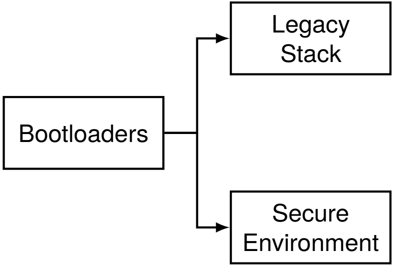
Bootloaders

Legacy Stack

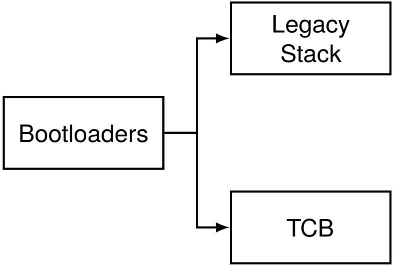
reset

Secure Environment

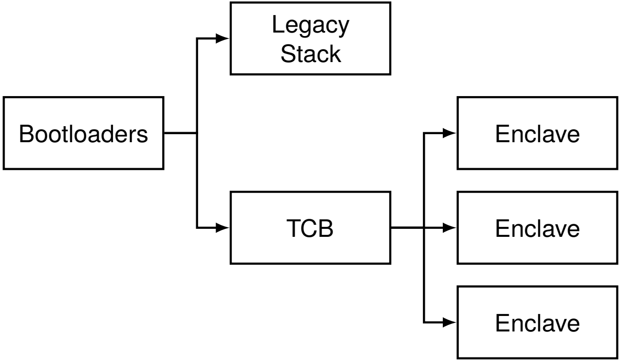
TCB



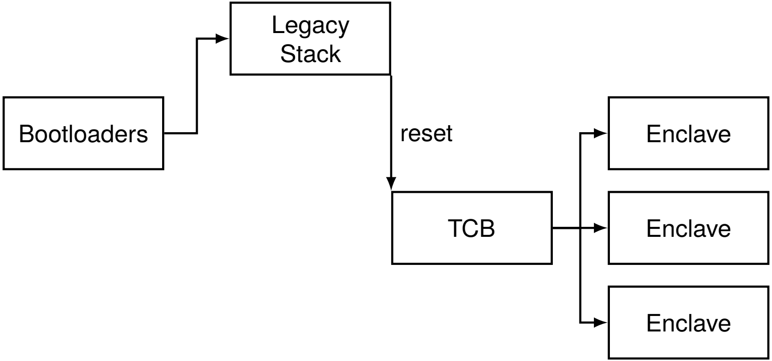
TCB



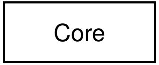
TCB



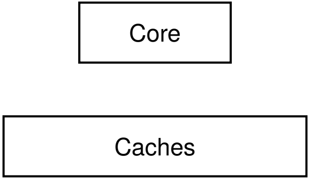
Dynamic Booted TCB



What to Isolate?



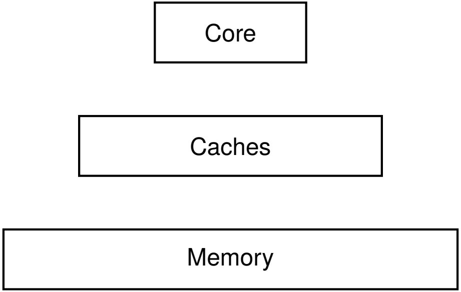
What to Isolate?



Core

Caches

What to Isolate?

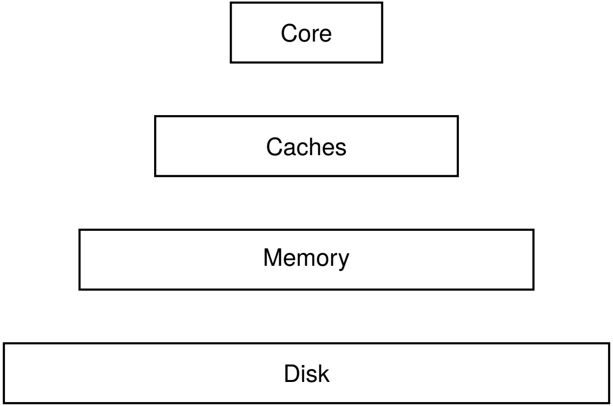


Core

Caches

Memory

What to Isolate?



Core

Caches

Memory

Disk

Isolation Strategies

Temporal partitioning

Isolation Strategies

Temporal partitioning

Resource

Isolation Strategies

Temporal partitioning

Isolation Strategies

Temporal partitioning

Resource

Isolation Strategies

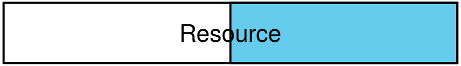
Temporal partitioning

Spatial partitioning

Isolation Strategies

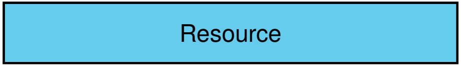
Temporal partitioning

Spatial partitioning

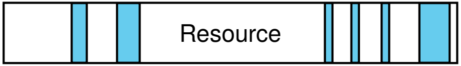


Isolation Strategies

Temporal partitioning

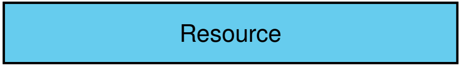


Spatial partitioning



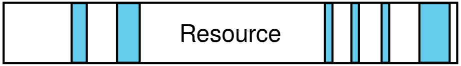
Isolation Strategies

Temporal partitioning



Resource

Spatial partitioning



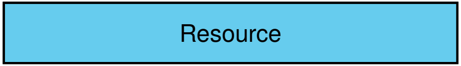
Resource

Spatio-Temporal partitioning

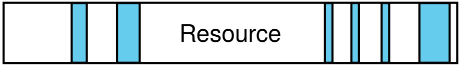
Resource

Isolation Strategies

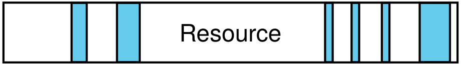
Temporal partitioning



Spatial partitioning

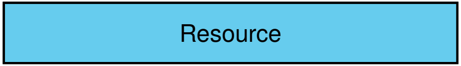


Spatio-Temporal partitioning

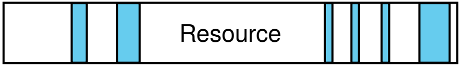


Isolation Strategies

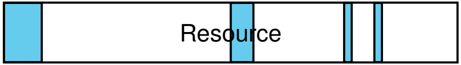
Temporal partitioning



Spatial partitioning

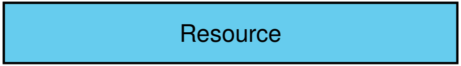


Spatio-Temporal partitioning

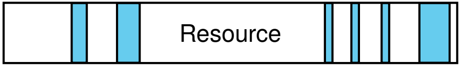


Isolation Strategies

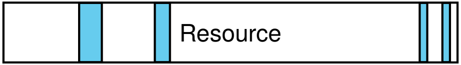
Temporal partitioning



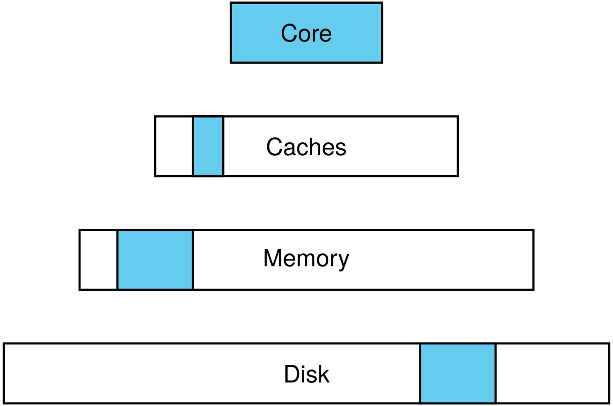
Spatial partitioning



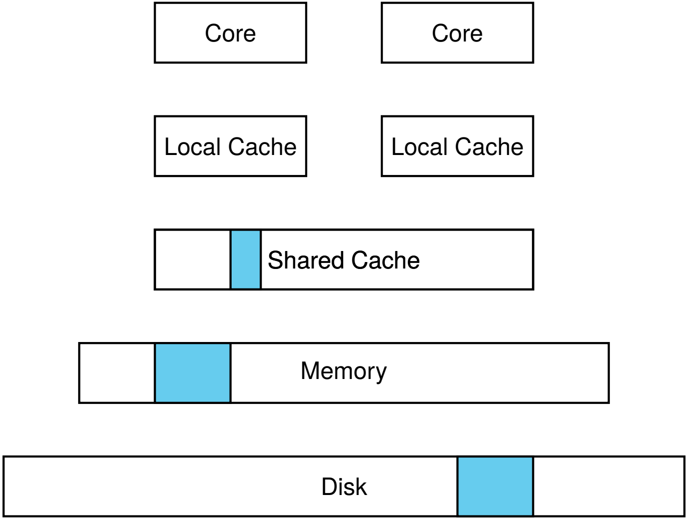
Spatio-Temporal partitioning



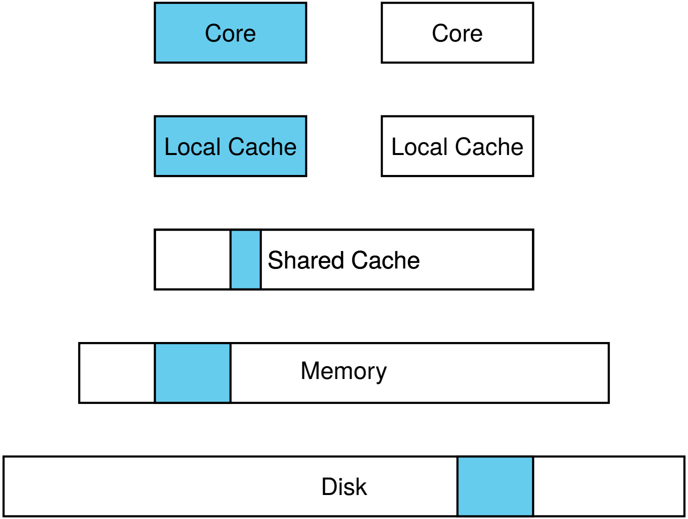
Isolation Strategy Example I



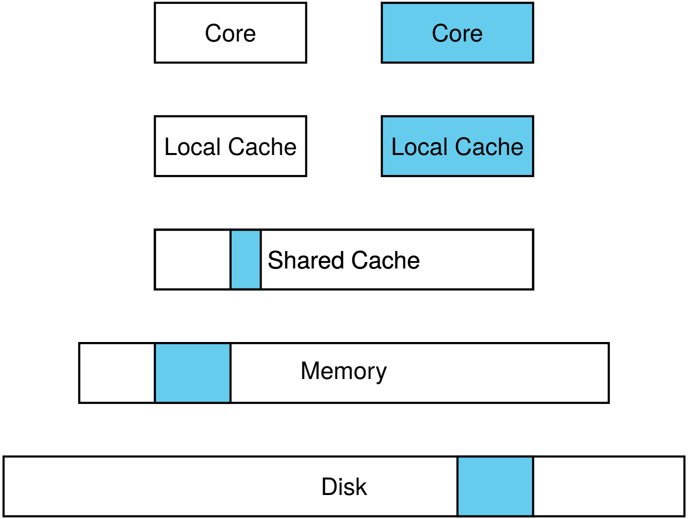
Isolation Strategy Example II



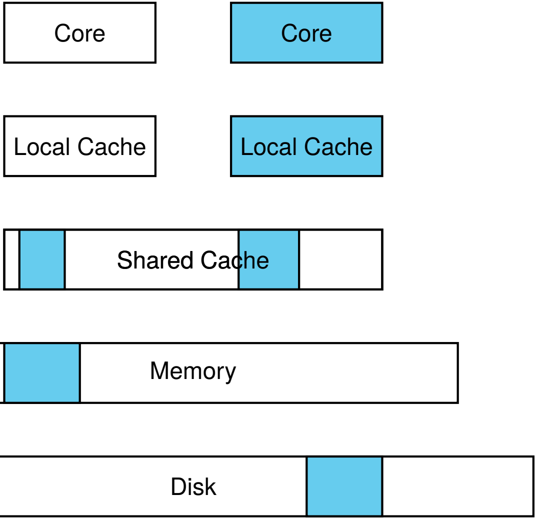
Isolation Strategy Example II



Isolation Strategy Example II



Isolation Strategy Example II

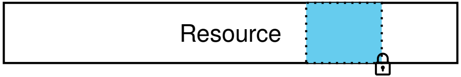


Isolation Enforcement

Cryptographic Enforcement:

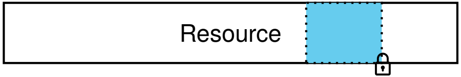
Isolation Enforcement

Cryptographic Enforcement:



Isolation Enforcement

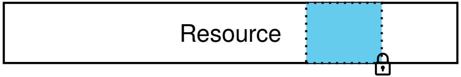
Cryptographic Enforcement:



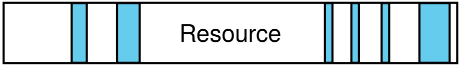
Logical Enforcement:

Isolation Enforcement

Cryptographic Enforcement:

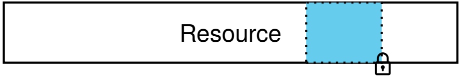


Logical Enforcement:

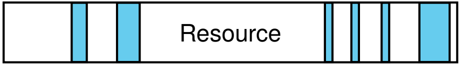


Isolation Enforcement

Cryptographic Enforcement:



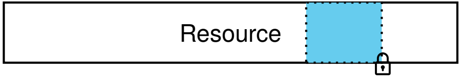
Logical Enforcement:



- Accesses always succeed
- Confidentiality through encryption
- Integrity through MACs/MerkleTrees

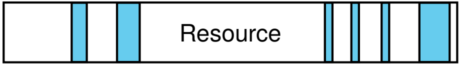
Isolation Enforcement

Cryptographic Enforcement:



- Accesses always succeed
- Confidentiality through encryption
- Integrity through MACs/MerkleTrees

Logical Enforcement:



- Access policy enforced by hardware
- Confidentiality and Integrity guaranteed

Core Isolation

	Name	Isol Strat	Privilege Level	
			Enclave	Software TCB
Industry	Intel SGX [23, 2]	T-L	App	-
	Intel TDX [8]	T-L	VM	PL1
	AMD SEV-SNP[17]	T-L	VM	-
	ARM TZ[1]	T-L	App/VM	PL0+(PL1/2)
	ARM CCA [3]	T-L	VM	PL0+(PL1)
	IBM PEF [14]	T-L	VM	PL0
Academia	Flicker [21]	T-L	VM	-
	SEA [22]	T-L	VM	-
	SICE [4]	T-L	VM	PL0
	PodArch [26]	T-L	App	-
	HyperCoffer [32]	T-L	VM	PL0
	H-SVM [15, 16]	T-L	VM	-
	EqualVisor [10]	T-L	VM	PL1
	xu-cc15 [33]	T-L	App	-
	wen-cf13 [31]	T-L	VM	-
	Komodo [13]	T-L	App	PL0 + PL2
	SANCTUARY [6]	T-L	App	PL0 + PL2
	TrustICE [28]	T-L	App	PL0 + PL2
	HA-VMSI [34]	T-L	VM	PL0
	Sanctum [9]	T-L	App	PL0
	TIMBER-V [30]	T-L	App	PL0
	Keystone [19]	T-L	App	PL0
	Penglai [12]	T-L	App	PL0
	CURE [5]	T-L	App/VM	PL0
	Iso-X [11]	T-L	App	-
	HyperWall [29]	T-L	VM	-
	Sancus [25, 24]	T-L	App	-
	TrustLite [18]	T-L	App	PL0
	TyTan [7]	T-L	App	PL0
	XOM [20]	T-L	App	-
	AEGIS [27]	T-L	App	-

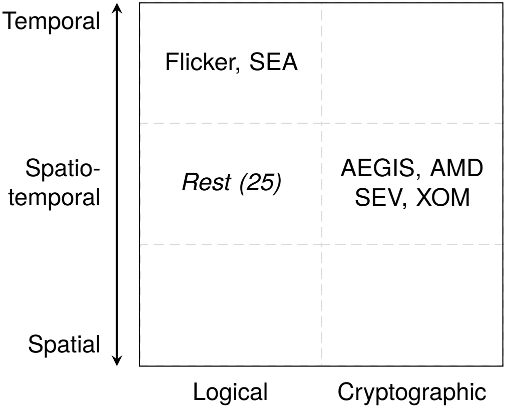
Core Isolation

	Name	Isol Strat	Privilege Level	
			Enclave	Software TCB
Industry	Intel SGX [23, 2]	T-L	App	-
	Intel TDX [8]	T-L	VM	PL1
	AMD SEV-SNP[17]	T-L	VM	-
	ARM TZ[1]	T-L	App/VM	PL0+(PL1/2)
	ARM CCA [3]	T-L	VM	PL0+(PL1)
	IBM PEF [14]	T-L	VM	PL0
Academia	Flicker [21]	T-L	VM	-
	SEA [22]	T-L	VM	-
	SICE [4]	T-L	VM	PL0
	PodArch [26]	T-L	App	-
	HyperCoffer [32]	T-L	VM	PL0
	H-SVM [15, 16]	T-L	VM	-
	EqualVisor [10]	T-L	VM	PL1
	xu-cc15 [33]	T-L	App	-
	wen-cf13 [31]	T-L	VM	-
	Komodo [13]	T-L	App	PL0 + PL2
	SANCTUARY [6]	T-L	App	PL0 + PL2
	TrustICE [28]	T-L	App	PL0 + PL2
	HA-VMSI [34]	T-L	VM	PL0
	Sanctum [9]	T-L	App	PL0
	TIMBER-V [30]	T-L	App	PL0
	Keystone [19]	T-L	App	PL0
	Penglai [12]	T-L	App	PL0
	CURE [5]	T-L	App/VM	PL0
	Iso-X [11]	T-L	App	-
	HyperWall [29]	T-L	VM	-
	Sancus [25, 24]	T-L	App	-
	TrustLite [18]	T-L	App	PL0
	TyTan [7]	T-L	App	PL0
	XOM [20]	T-L	App	-
	AEGIS [27]	T-L	App	-

Memory Isolation

	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	AEGIS, AMD SEV, XOM
Spatial		

Memory Isolation *against a Software Adversary**



	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	AEGIS, AMD SEV, XOM
Spatial		

Cache Isolation

	Logical	Cryptographic
Temporal	CURE, Flicker, Sanctum, SEA	
Spatio-temporal	*Rest (26)*	
Spatial	Penglai	

(a) Local Cache

	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	
Spatial	CURE, Keystone, Penglai, Sanctum	

(b) Shared Cache

Cache Isolation *against a Software Adversary**

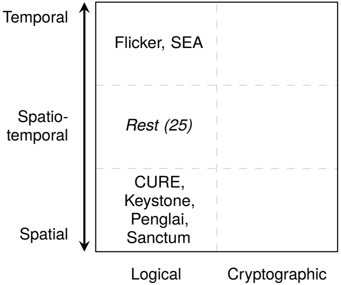
	Logical	Cryptographic
Temporal	CURE, Flicker, Sanctum, SEA	
Spatio-temporal	*Rest (26)*	
Spatial	Penglai	

(a) Local Cache

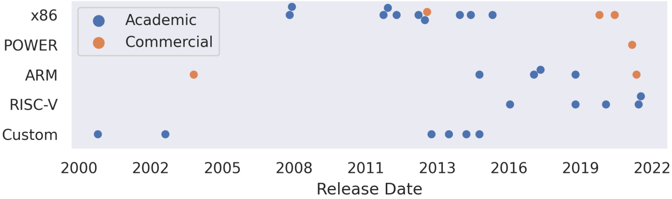
	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	
Spatial	CURE, Keystone, Penglai, Sanctum	

(b) Shared Cache

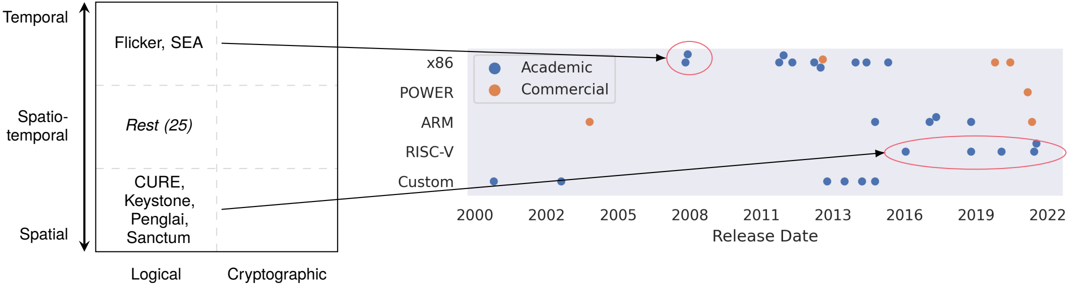
Shared Cache Isolation over Time



	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	
Spatial	CURE, Keystone, Penglai, Sanctum	



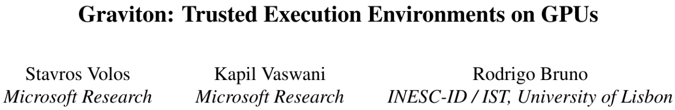
Shared Cache Isolation over Time



Memory Isolation against a Physical Adversary

	Logical	Cryptographic
Temporal		
Spatio-temporal		*All (10)*
Spatial		

What about other Devices?



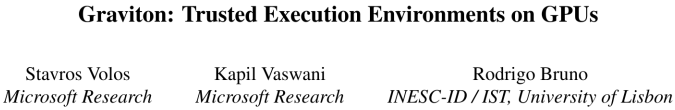
Graviton: Trusted Execution Environments on GPUs

Stavros Volos
Microsoft Research

Kapil Vaswani
Microsoft Research

Rodrigo Bruno
INESC-ID / IST, University of Lisbon

What about other Devices?

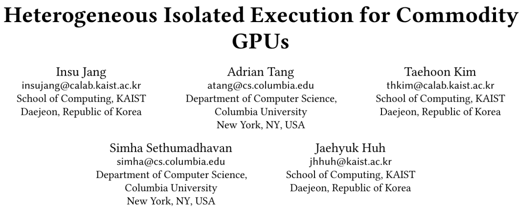


Graviton: Trusted Execution Environments on GPUs

Stavros Volos
Microsoft Research

Kapil Vaswani
Microsoft Research

Rodrigo Bruno
INESC-ID / IST, University of Lisbon



Heterogeneous Isolated Execution for Commodity GPUs

Insu Jang
insujang@calab.kaist.ac.kr
School of Computing, KAIST
Daejeon, Republic of Korea

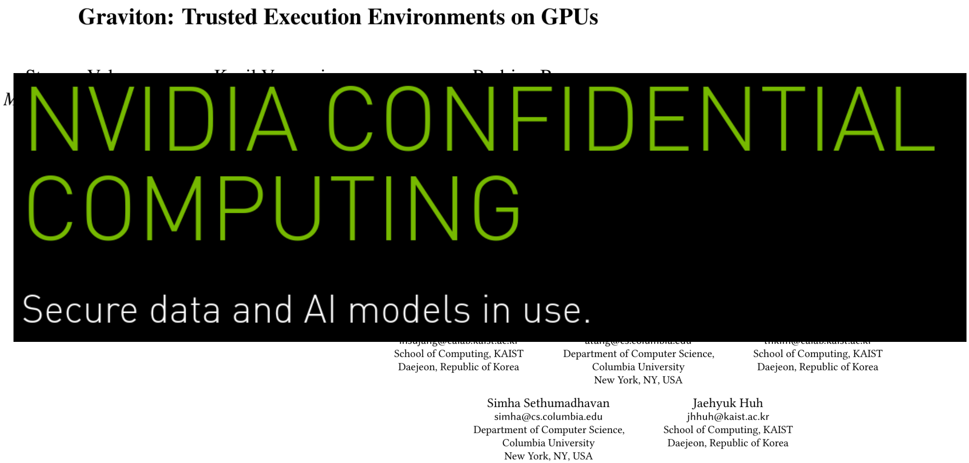
Adrian Tang
atang@cs.columbia.edu
Department of Computer Science,
Columbia University
New York, NY, USA

Taehoon Kim
thkim@calab.kaist.ac.kr
School of Computing, KAIST
Daejeon, Republic of Korea

Simha Sethumadhavan
simha@cs.columbia.edu
Department of Computer Science,
Columbia University
New York, NY, USA

Jaehyuk Huh
jhhuh@kaist.ac.kr
School of Computing, KAIST
Daejeon, Republic of Korea

What about other Devices?



Graviton: Trusted Execution Environments on GPUs

NVIDIA CONFIDENTIAL COMPUTING

Secure data and AI models in use.

School of Computing, KAIST
Daejeon, Republic of Korea

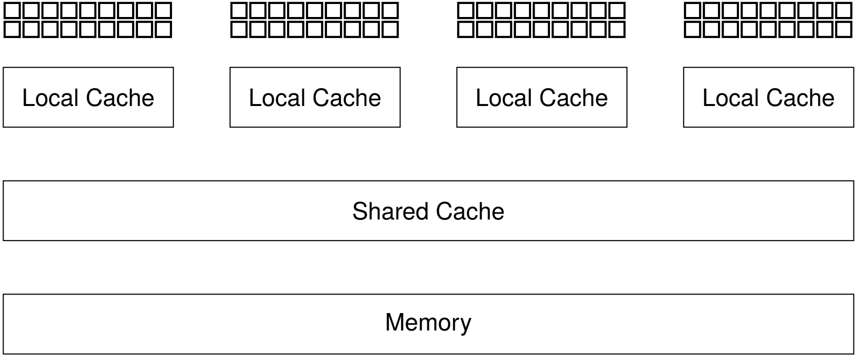
Department of Computer Science,
Columbia University
New York, NY, USA

School of Computing, KAIST
Daejeon, Republic of Korea

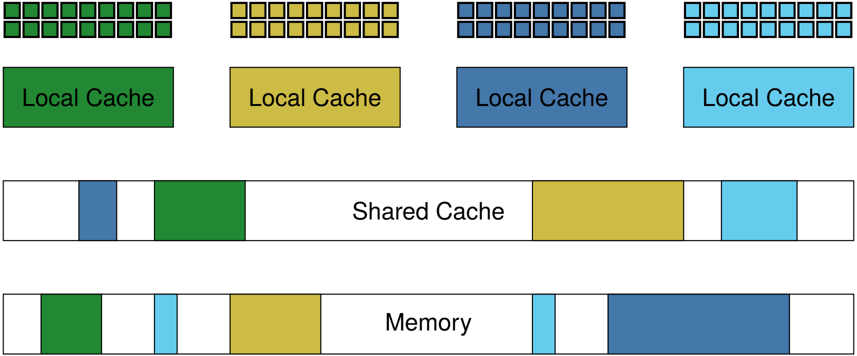
Simha Sethumadhavan
simha@cs.columbia.edu
Department of Computer Science,
Columbia University
New York, NY, USA

Jaehyuk Huh
jhhuh@kaist.ac.kr
School of Computing, KAIST
Daejeon, Republic of Korea

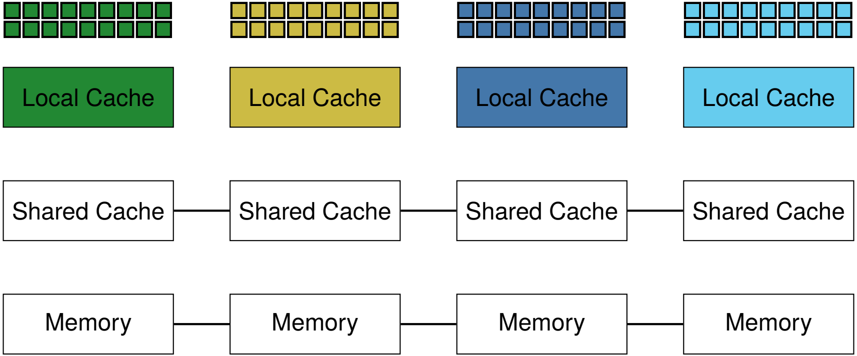
Isolation on Nvidia GPUs



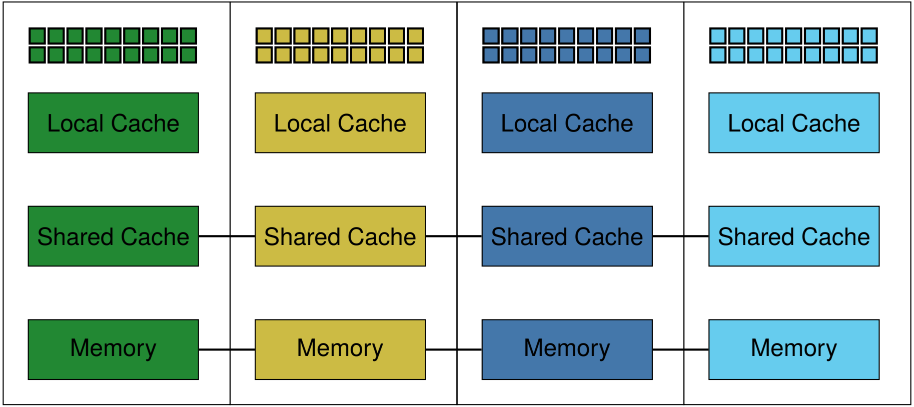
Isolation on Nvidia GPUs



Isolation on Nvidia GPUs



Isolation on Nvidia GPUs



Cache Isolation Strategies

	Logical	Cryptographic
Temporal	CURE, Flicker, Sanctum, SEA	
Spatio-temporal	*Rest (26)*	
Spatial	Penglai, **NVIDIA**	

(a) Local Cache

	Logical	Cryptographic
Temporal	Flicker, SEA	
Spatio-temporal	*Rest (25)*	
Spatial	CURE, Keystone, Penglai, Sanctum, **NVIDIA**	

(b) Shared Cache

Are we done?

- CPU TEEs largely figured out

Are we done?

- CPU TEEs largely figured out
    - A lot of reinvention

Are we done?

- CPU TEEs largely figured out
  - A lot of reinvention
  - How to increase transparency?

Are we done?

- CPU TEEs largely figured out
  - A lot of reinvention
  - How to increase transparency?
  - Performance improvements still possible

Are we done?

- CPU TEEs largely figured out
  - A lot of reinvention
  - How to increase transparency?
  - Performance improvements still possible
- TEEs on different architectures still in its infancy

Are we done?

- CPU TEEs largely figured out
  - A lot of reinvention
  - How to increase transparency?
  - Performance improvements still possible
- TEEs on different architectures still in its infancy
- How to combine TEEs on multiple devices?