基于硬件可信执行环境的隐私计算

王文浩

中国科学院信息工程研究所

提纲

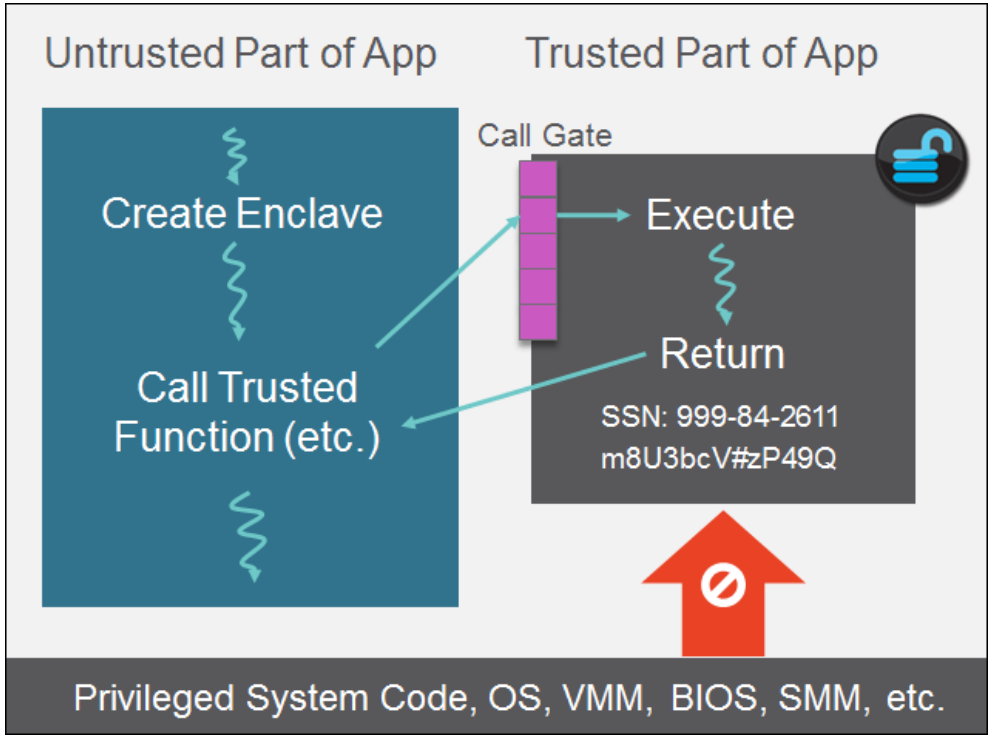
- 隐私计算与可信执行环境 TEE
- Intel SGX
- SGX 的不足及可能的解决思路
- 其它 TEE
- 总结

隐私计算

- 数据和计算来自同一个参与方
  - 外包计算
- 数据和计算来自两个参与方
  - Machine Learning as A Service
- 数据来自两个（或）多个参与方
  - 联合机器模型训练
- ……

可信执行环境 TEE

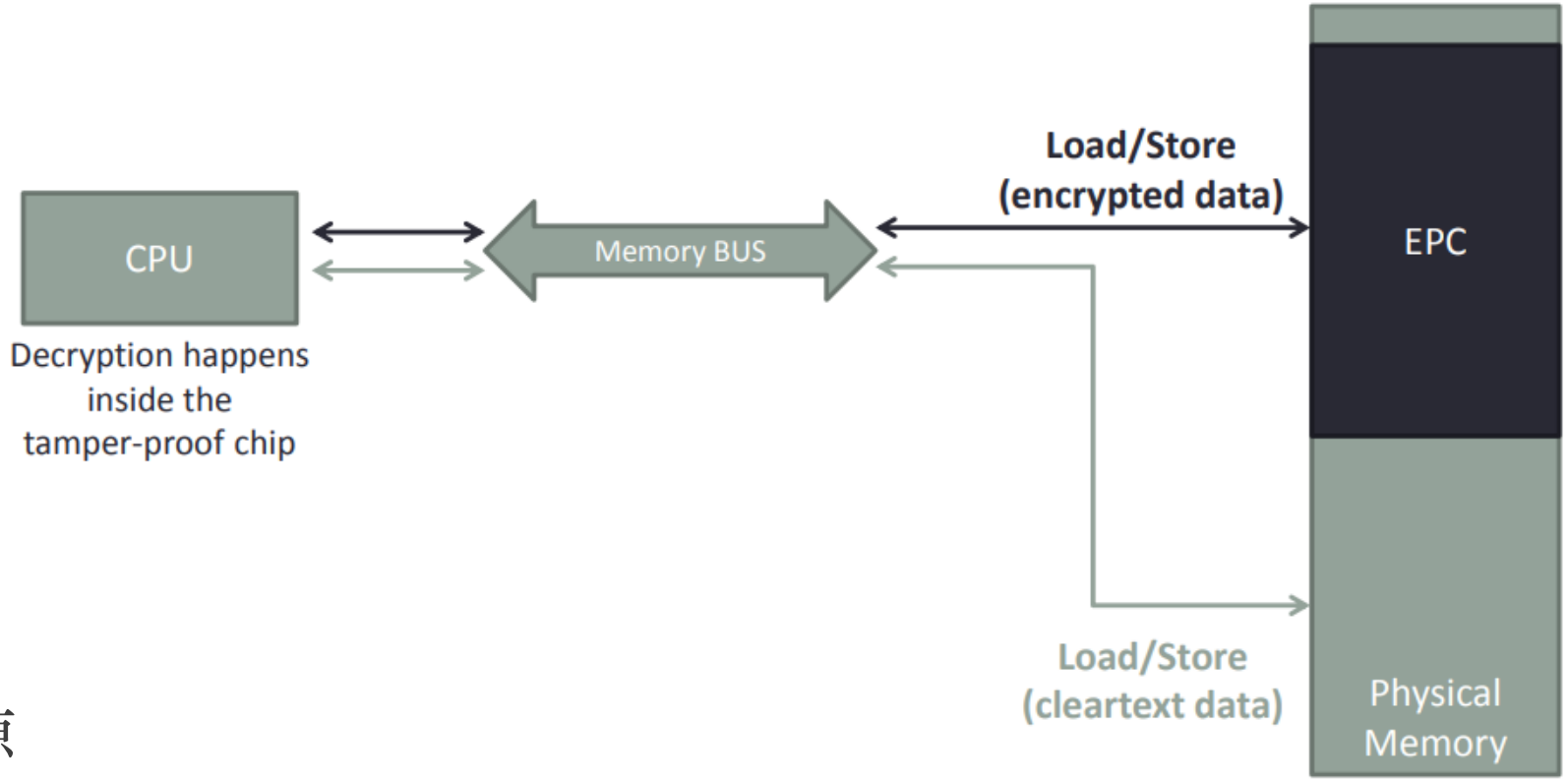
- 隔离
  - 隔离的内存和计算资源
  - 不会被未经授权的访问或篡改
- Attestation
  - 向远程用户证明自己的身份
  - 合法的硬件、正确的软件
- Sealing
  - Persisting secret



INTEL SGX

Intel 公司的 TEE 的实现

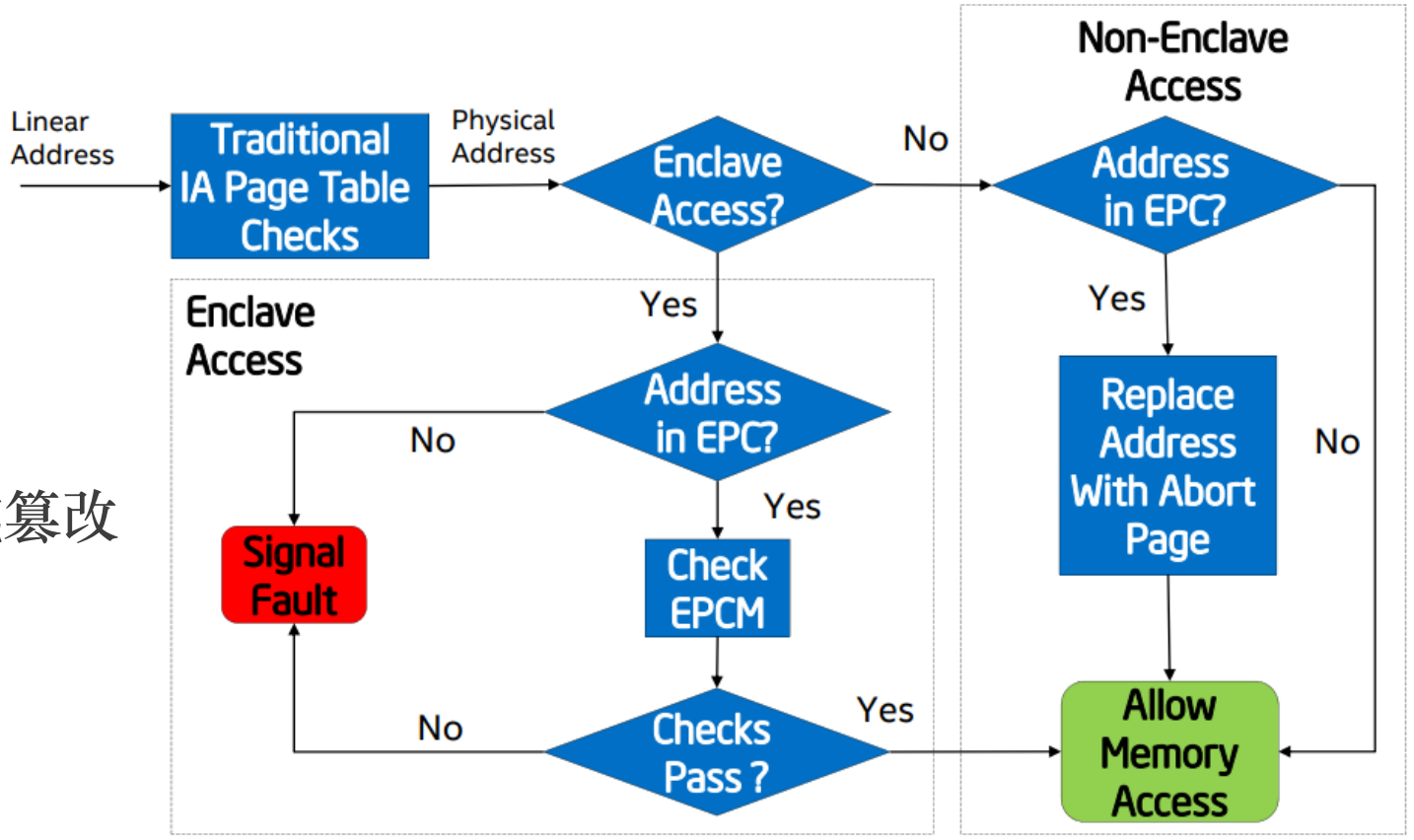
- x86 指令集扩展
- Native performance
- 商用
- Small TCB



- 隔离 **物理**
  - 隔离的内存和计算资源
  - 不会被未经授权的访问或篡改

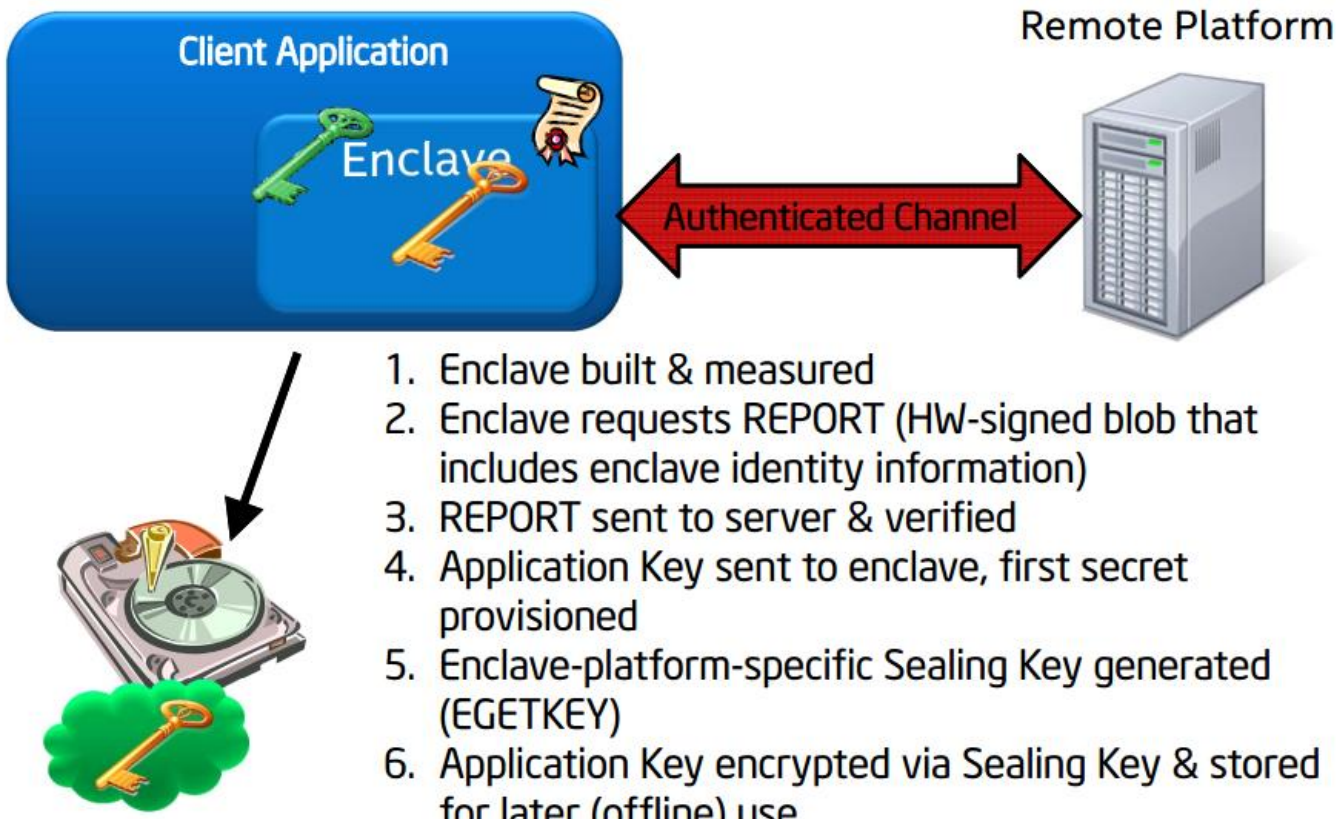
INTEL SGX

- 隔离 **虚拟**
  - 隔离的内存和计算资源
  - 不会被未经授权的访问或篡改



INTEL SGX

- Attestation
  - 向远程用户证明自己的身份
  - 合法的硬件、正确的软件
- Sealing
  - Persisting secret



SGX 可以试图解决的问题

加密数据库

EnclaveDB – A Secure Database using SGX

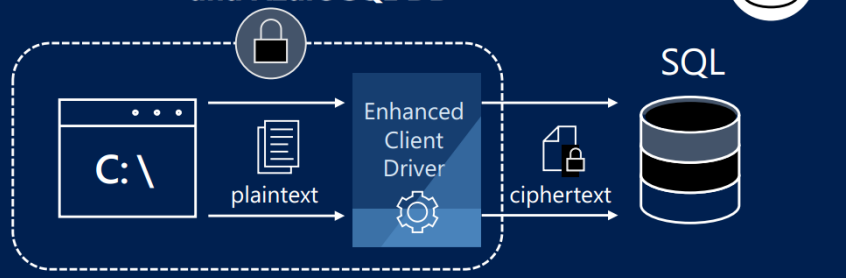
Christian Priebe, Kapil Vaswani, Manuel Costa

To appear in the Proceedings of the IEEE Symposium on Security & Privacy, May 2018 | May 2018

SQL Always Encrypted

Protects sensitive data in use from high-privileged yet unauthorized SQL users both on-premises and in the cloud

Current GA version in SQL Server 2016/17 and Azure SQL DB



Client side Encryption

Client-side encryption of sensitive data using keys that are *never* given to the database system

Encryption Transparency

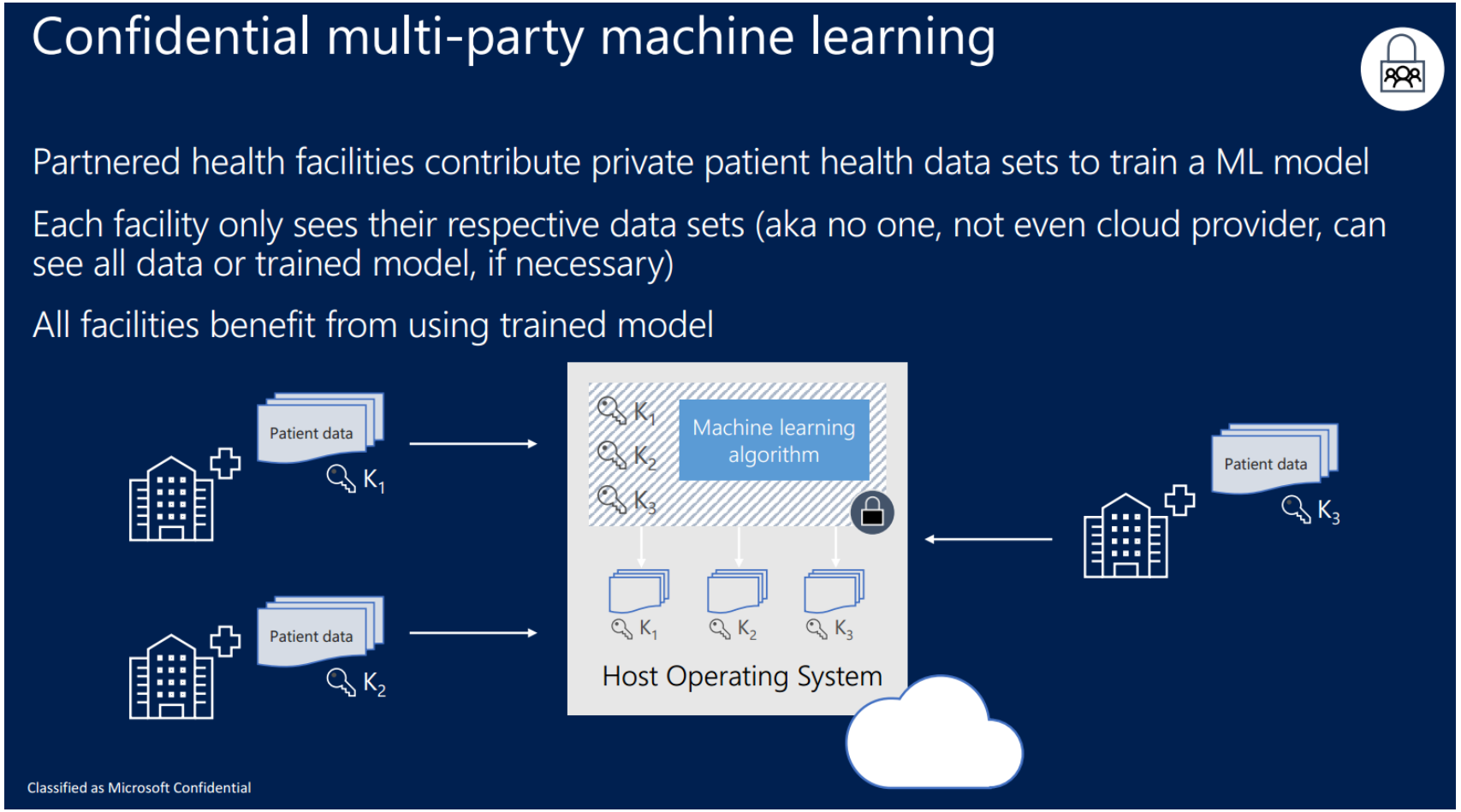
Client driver transparently encrypts query parameters and decrypts encrypted results

Queries on Encrypted Data

Support for equality comparison, including join, group by and distinct operators via deterministic encryption

SGX 可以试图解决的问题

联合机器模型训练



SGX 的不足

- 计算能力弱
- 侧信道问题
- Function Privacy
- Memory Safety

SGX 的不足

- 计算能力弱
- 侧信道问题
- Function Privacy
- Memory Safety

SGX 的不足

计算能力弱：至多8核，128 MB（or 256 MB）加密内存

Product Name	Status	Launch Date	# of Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP	Processor Graphics ‡	Compare All | None
Intel® Xeon® E-2278GEL Processor	Launched	Q2'19	8	3.90 GHz	2.00 GHz	16 MB	35 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2278GE Processor	Launched	Q2'19	8	4.70 GHz	3.30 GHz	16 MB	80 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2176G Processor	Launched	Q3'18	6	4.70 GHz	3.70 GHz	12 MB SmartCache	80 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2186G Processor	Launched	Q3'18	6	4.70 GHz	3.80 GHz	12 MB SmartCache	95 W	Intel® UHD Graphics P630	
Intel® Xeon® Processor E3-1240L v5	Launched	Q4'15	4	3.20 GHz	2.10 GHz	8			
Intel® Xeon® Processor E3-1280 v5	Launched	Q4'15	4	4.00 GHz	3.70 GHz	8			
Intel® Xeon® Processor E3-1220 v5	Launched	Q4'15	4	3.50 GHz	3.00 GHz	8			

Intel introduced the Intel SGX Card in February 2019. It is a new way to help extend application memory protections using Intel Software Guard Extensions in existing data center infrastructure. (Credit: Intel Corporation)

Intel SGX for the Data Center

Helping protect customer data in the cloud is a top priority for cloud service providers. Intel® Software Guard Extensions (Intel® SGX) was designed to help create more secure environments without having to trust the integrity of all the layers of the system. The technology isolates specific application code and data to run in private regions of memory, or enclaves. Intel SGX is currently used by top cloud providers, including Alibaba Cloud*, Baidu*, IBM Cloud Data Guard* and Microsoft Azure* for various projects to help protect customer data at runtime. Today, Intel announced new products and ecosystem solutions that enable Intel SGX to be used even more broadly in the data center.

More: RSA 2019

Scaling Intel SGX for the Cloud: Intel introduced the Intel SGX Card, a new way to help extend application memory protections using Intel SGX in existing data center infrastructure. Though Intel SGX technology will be available on future multi-socket Intel® Xeon® Scalable processors, there is pressing demand for its security benefits in this space today. Intel is accelerating deployment of Intel SGX technology for the vast majority of cloud servers deployed today with the Intel SGX Card. Additional benefits offer access to larger, non-enclave memory spaces, and some additional side-channel protections when compartmentalizing sensitive data to a separate processor and associated cache. Availability is targeted for later this year.

SGX 的不足

计算能力弱：至多8核，128 MB（or 256 MB）加密内存

扩展 TEE 至 GPU、FPGA 及 AI 加速器芯片等

Graviton: Trusted Execution Environments on GPUs

Stavros Volos and Kapil Vaswani, *Microsoft Research;*
Rodrigo Bruno, *INESC-ID / IST, University of Lisbon*

https://www.usenix.org/conference/osdi18/presentation/volos

This paper is included in the Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation (OSDI '18).
October 8–10, 2018 • Carlsbad, CA, USA
ISBN 978-1-931971-47-8

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

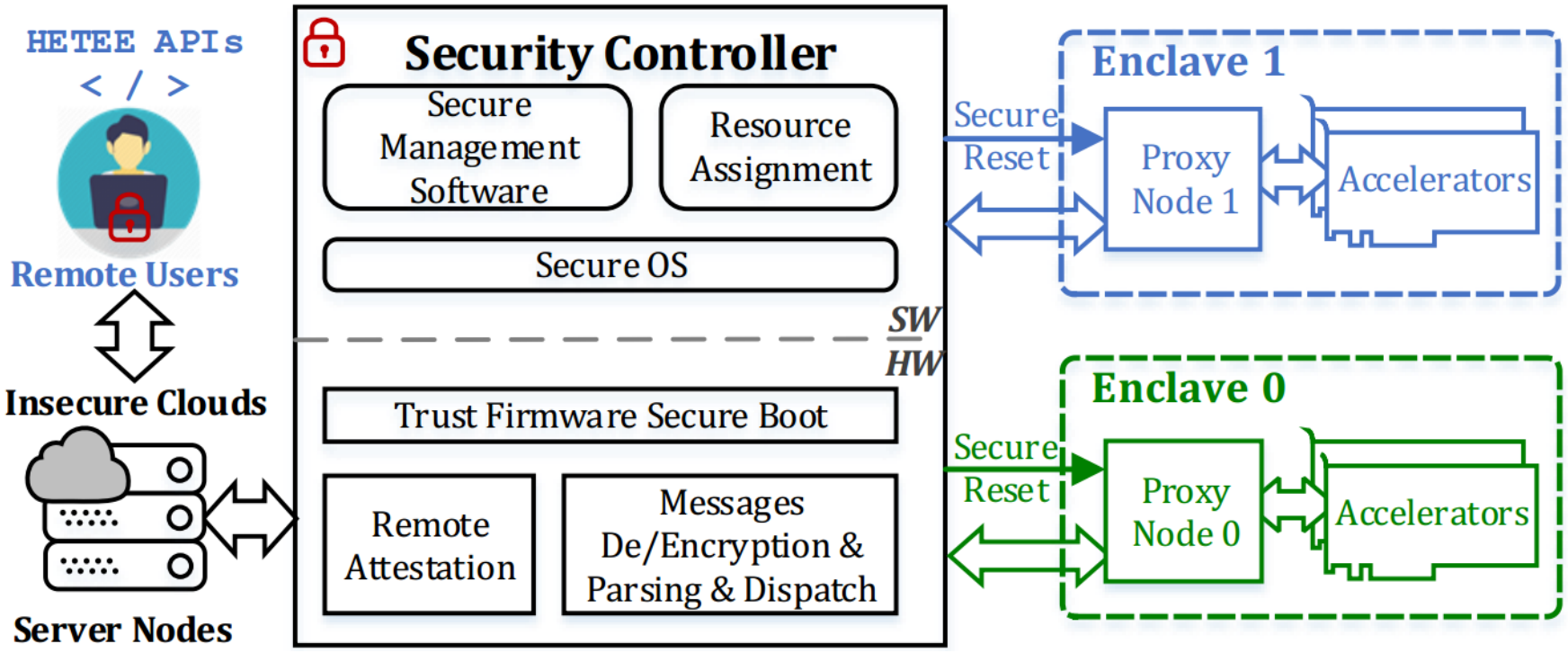
Simha Sethumadhavan
simha@cs.columbia.edu
Department of Computer Science,
Columbia University
New York, NY, USA

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

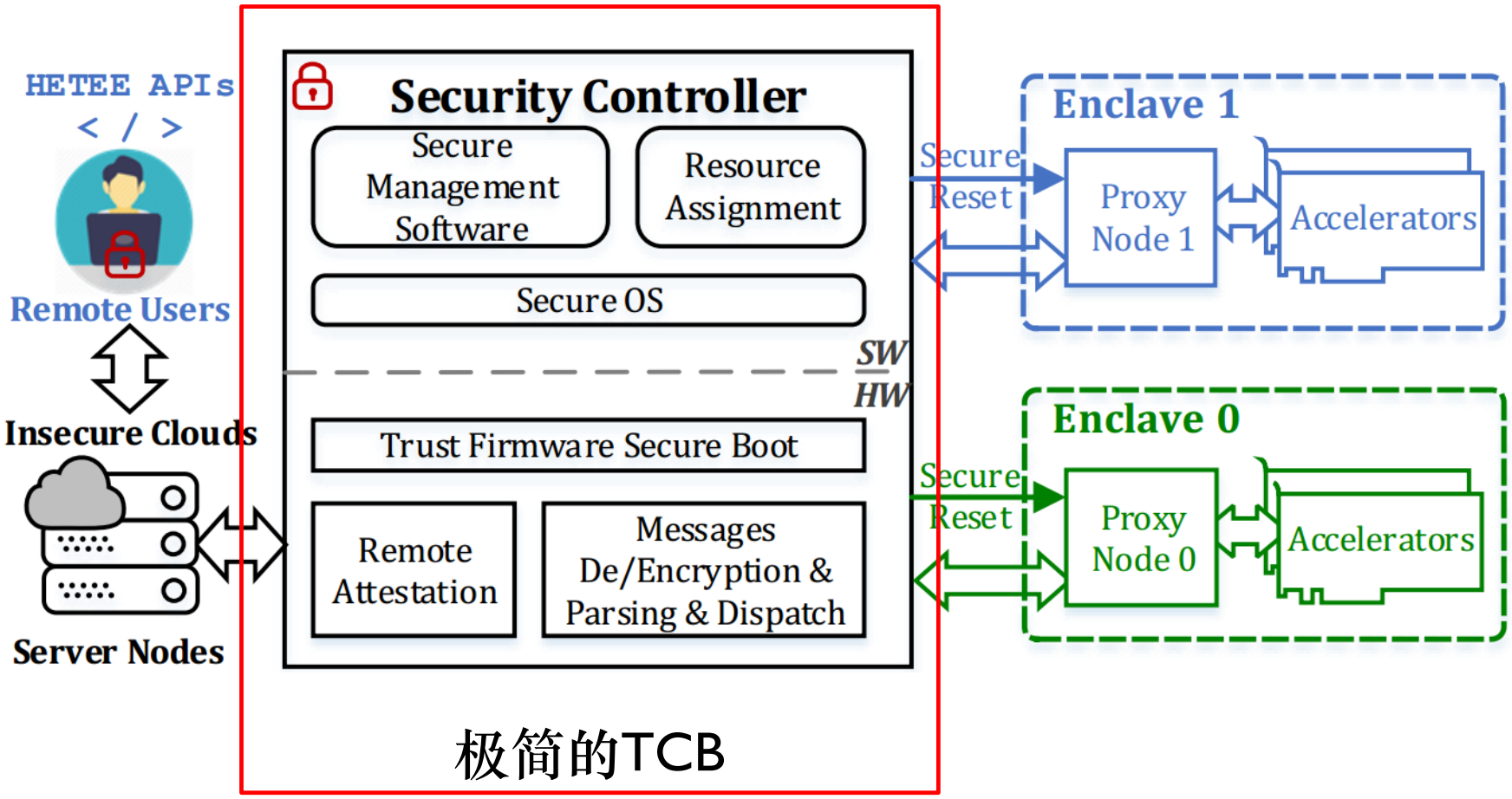
ASPLOS 2019

- 需要改GPU等硬件
- GPU runtime等heavy software stack需要在可信环境内
- GPU runtime和GPU的通信可能泄露侧信道信息
- 加解密的开销

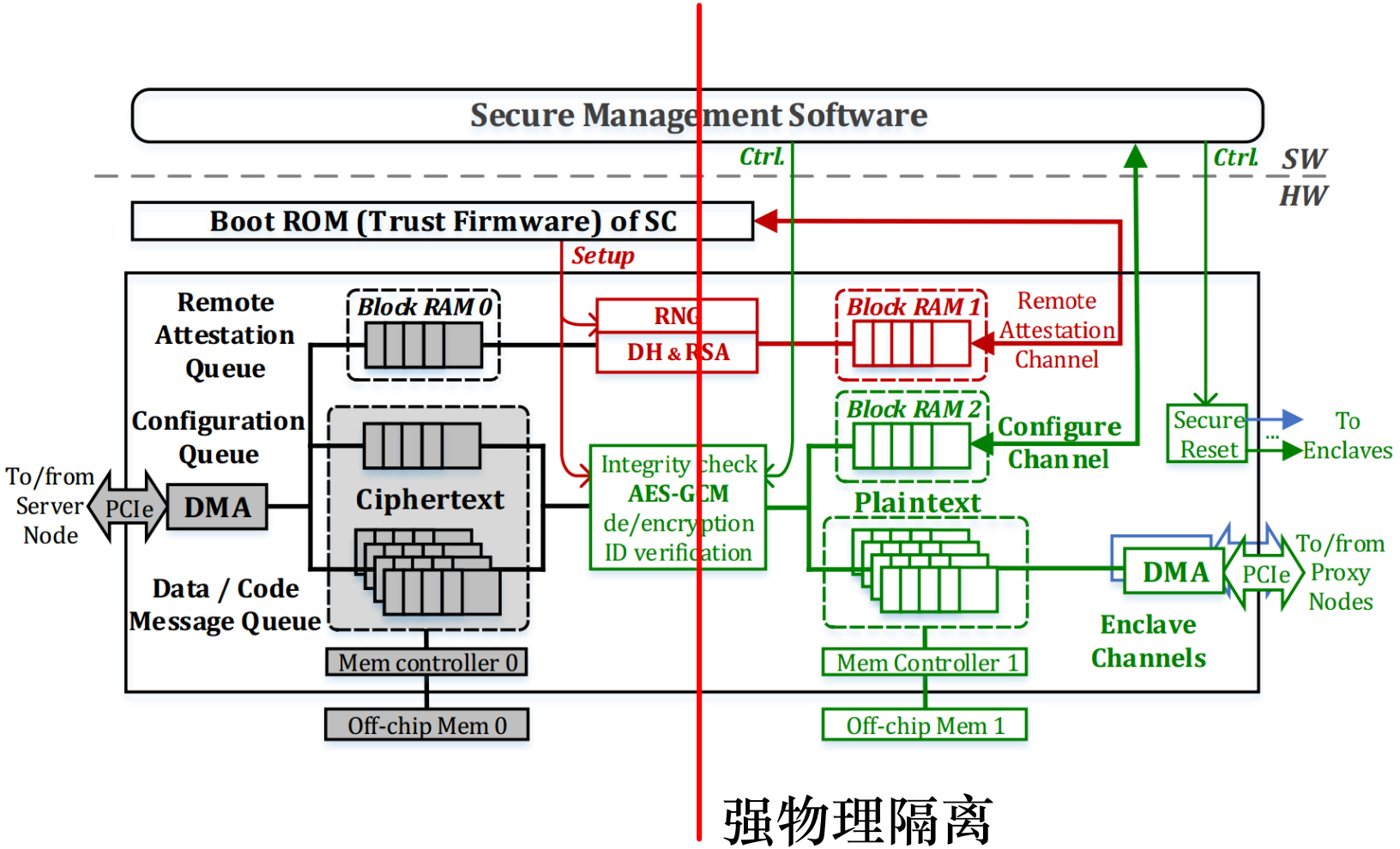
可能的解决思路：进展中的工作



可能的解决思路：进展中的工作



可能的解决思路：进展中的工作

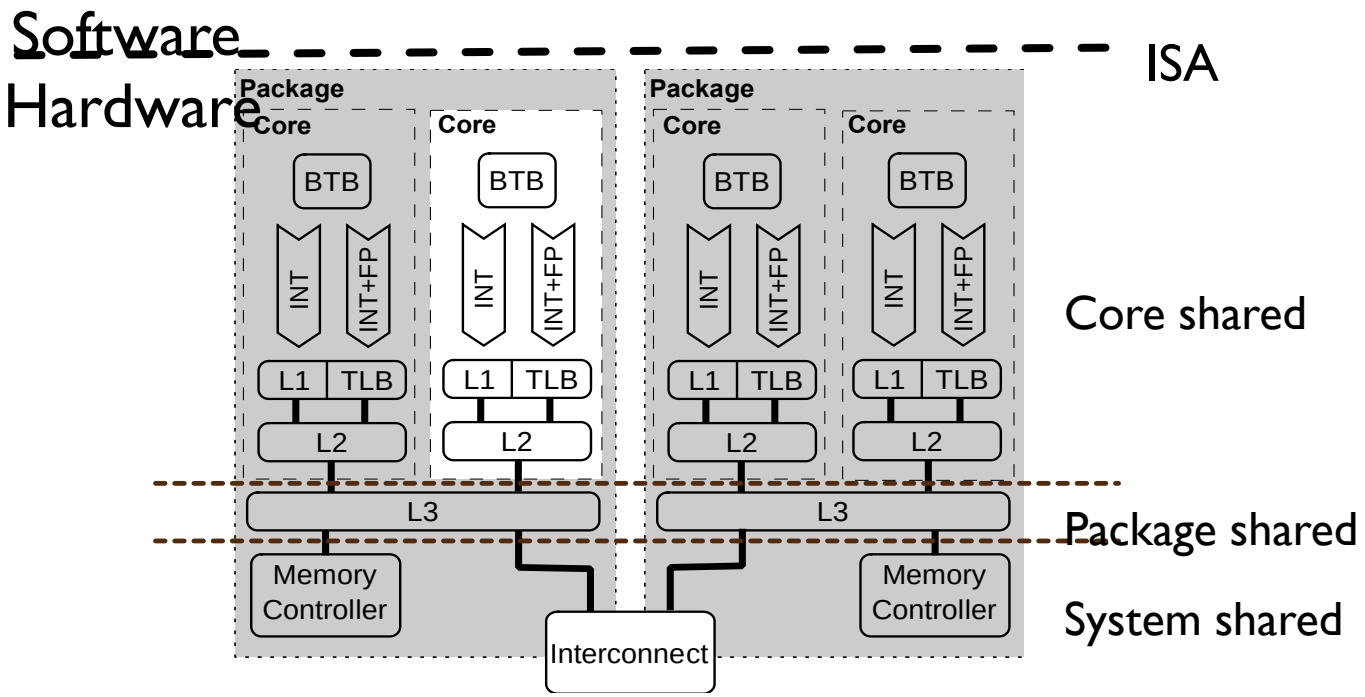


SGX 的不足

- 计算能力弱
- 侧信道问题
- Function Privacy
- Memory Safety

SGX 的不足

侧信道



类别	示例
页表	页表项P/A/D位（S&P 15, Usenix 17, CCS 17）
存储层次 Memory Hierarchy	多级cache、TLB、DRAM等缓存 (CCS 17)
功能单元竞争Function Unit Contention	Port contention (S&P 19)
功能单元状态Stateful Functional Units	Branch shadowing (Usenix 17)
Variable Instruction Execution Timing	Nemesis (CCS 18)
物理信号	电磁、功耗等

可能的解决思路

- 系统的角度
  - 检测异常中断
  - 检测cache eviction
  - 检测SMT（Hyper-Threading）
- 软件开发者的角度
  - Oblivious RAM
  - Oblivious program execution
  - Code/data randomization
- Side channel leakage modeling

可能的解决思路

- 系统的角度
  - 检测异常中断 (T-SGX、De javu)
  - 检测cache eviction (TSX, Usenix 18)
  - 检测SMT （HyperRace, SP 2018）
- 软件开发者的角度
  - Oblivious RAM
  - Oblivious program execution
  - Code/data randomization
- Side channel leakage modeling

类别	子类	State flushes on Context switches?	攻击假设或side effect	示例
Same-Core attack	功能单元状态	no	中断	BTB、BHT
		yes	SMT	Store buffer、line fill buffer
	功能单元竞争		中断或SMT	L1/L2缓存、TLB、port
Cross-Core Attack	cache		Cache eviction	LLC
	页表		中断	页表项P位
			中断或SMT	页表项A/D位

可能的解决思路

- 系统的角度
  - 检测异常中断 (T-SGX、De javu)
  - 检测cache eviction (TSX, Usenix 18)
  - 检测SMT （HyperRace, SP 2018）
- 软件开发者的角度
  - Oblivious RAM
  - Oblivious program execution
  - Code/data randomization
- Side channel leakage modeling

- ZeroTrace (NDSS 2018)
- OBLIVIATE: Oblivious File System (NDSS 2018)
- POSUP (PETS 2019)

- OBFUSCURO (NDSS 2019)

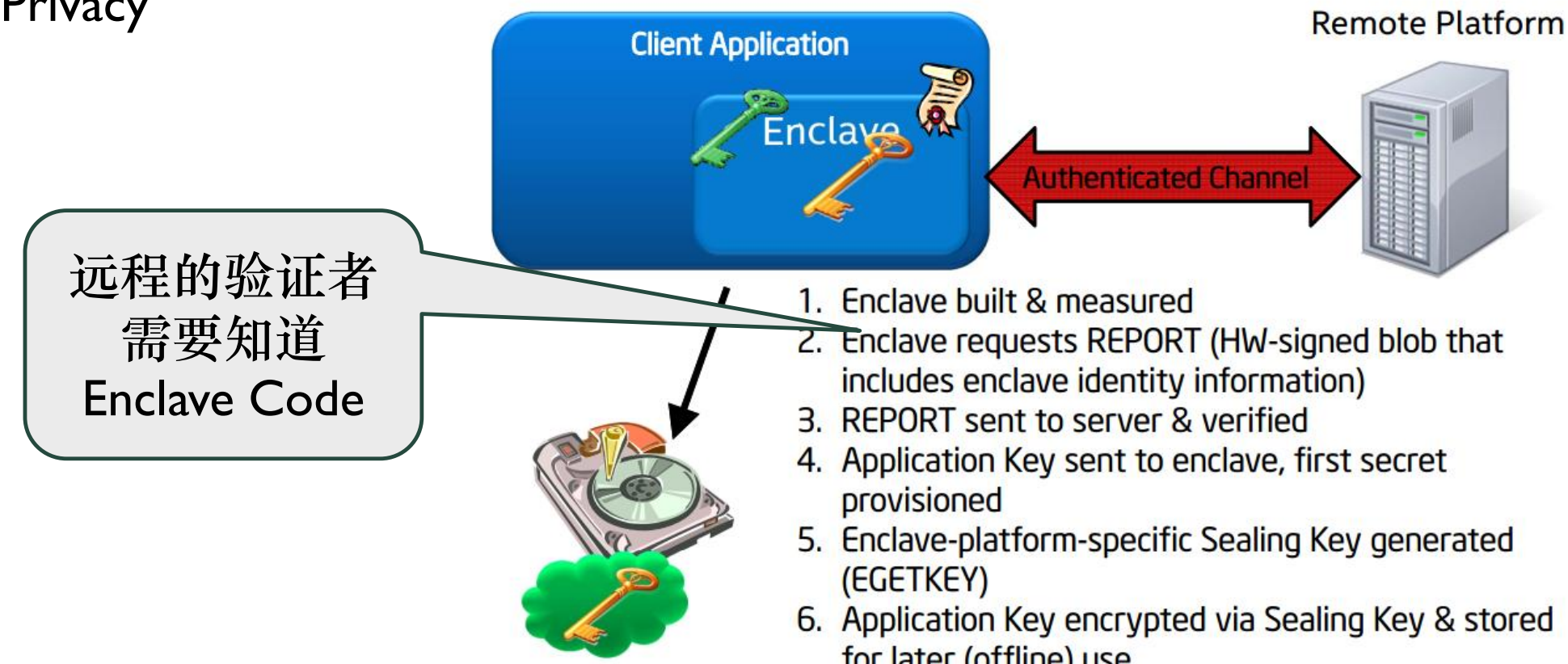
- SGX-Shield (NDSS 2017)
- Data randomization (ESORICS 2017)

SGX 的不足

- 计算能力弱
- 侧信道问题
- Function Privacy
- Memory Safety

SGX 的不足

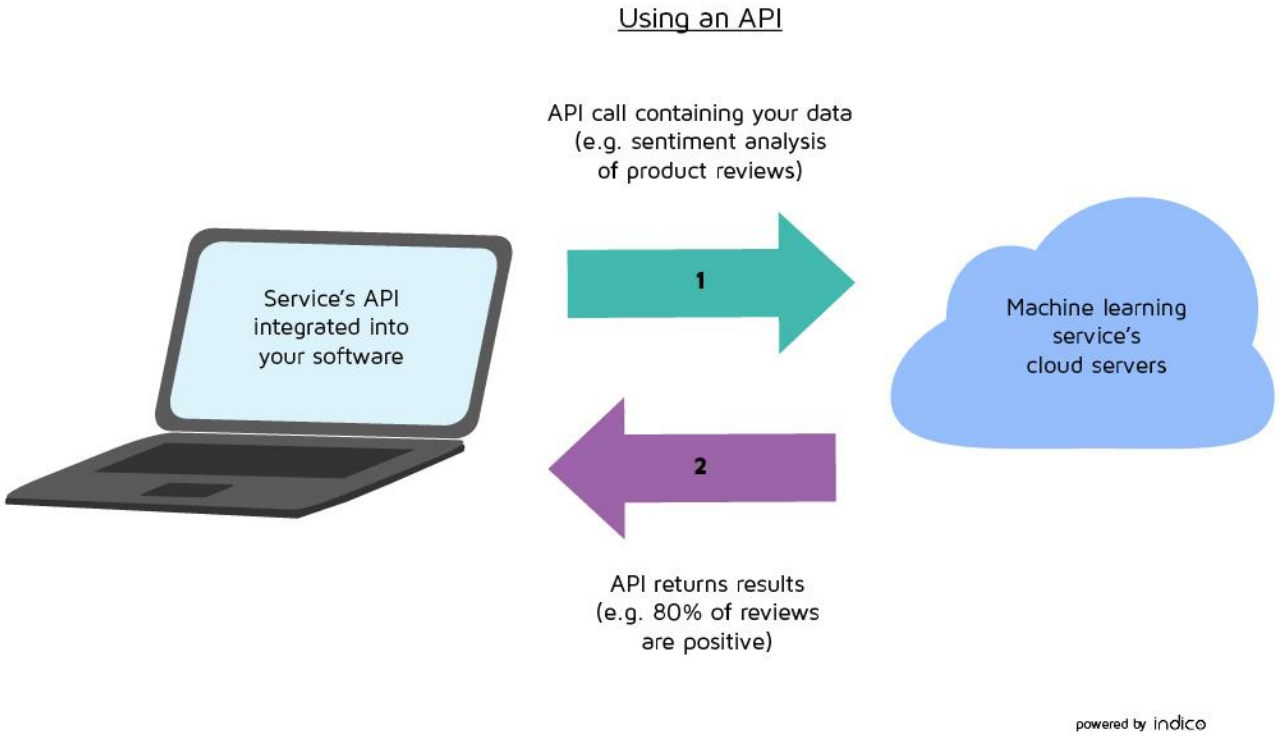
Function Privacy



可能的解决思路：进展中的工作

Function Privacy

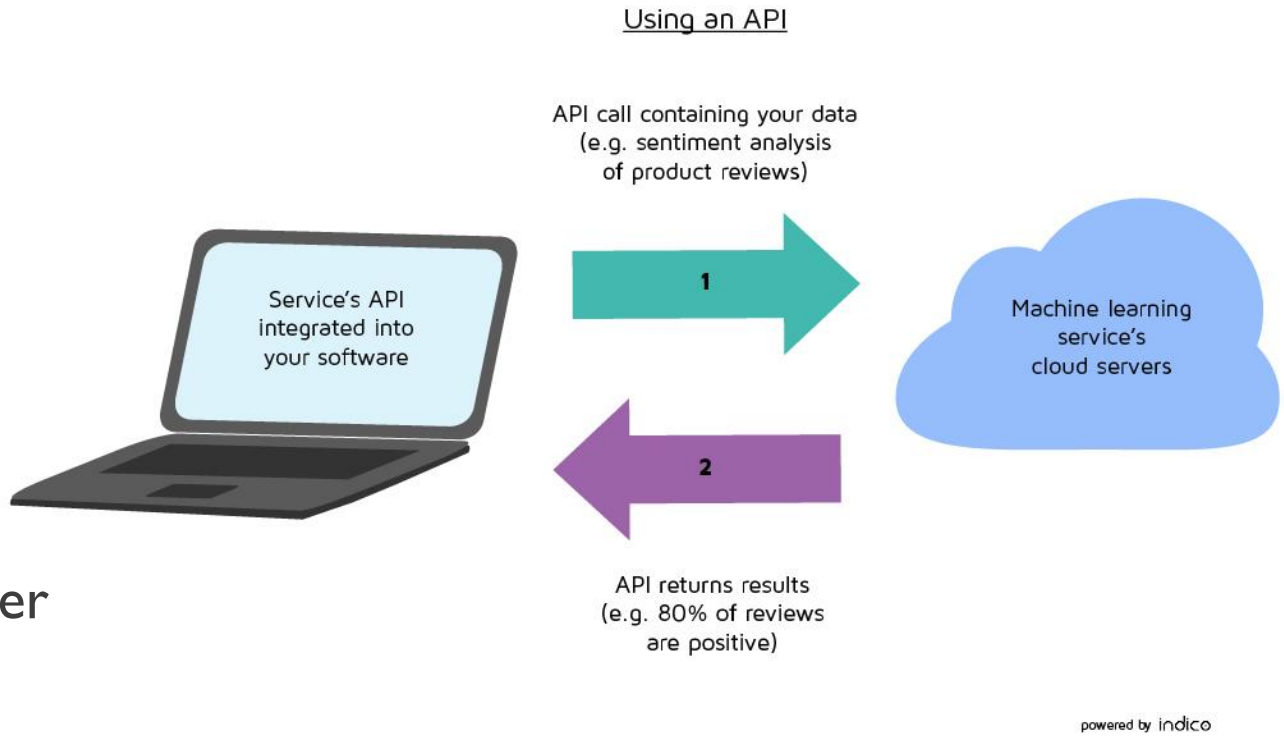
- 为证明自身，service provider需要向remote user展示自己的代码



可能的解决思路：进展中的工作

Function Privacy

- 为证明自身，service provider需要向remote user展示自己的代码



保证代码安全的认证：

- 在SGX内实现一个binary loader + checker
- 在SGX外提供编译器
- Checker检查代码，并向remote user提供证据
- 思路来源于proof carrying code（PCC）

SGX 的不足

- 计算能力弱
- 侧信道问题
- Function Privacy
- Memory Safety

SGX 的不足

Memory Safety

Hacking in Darkness: Return-oriented Programming against Secure Enclaves

Jaehyuk Lee and Jinsoo Jang, *KAIST;* Yeongjin Jang, *Georgia Institute of Technology;* Nohyun Kwak, Yeseul Choi, and Changho Choi, *KAIST;* Taesoo Kim, *Georgia Institute of Technology;* Marcus Peinado, *Microsoft Research;* Brent Byunghoon Kang, *KAIST*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/lee-jaehyuk

This paper is included in the Proceedings of the
26th USENIX Security Symposium

August 16–18, 2017 • Vancouver, BC, Canada

ISBN 978-1-931971-40-9

The Guard's Dilemma: Efficient Code-Reuse Attacks Against Intel SGX

Andrea Biondo and Mauro Conti, *University of Padua;* Lucas Davi, *University of Duisburg-Essen;* Tommaso Frassetto and Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*

https://www.usenix.org/conference/usenixsecurity18/presentation/biondo

This paper is included in the Proceedings of the
27th USENIX Security Symposium.

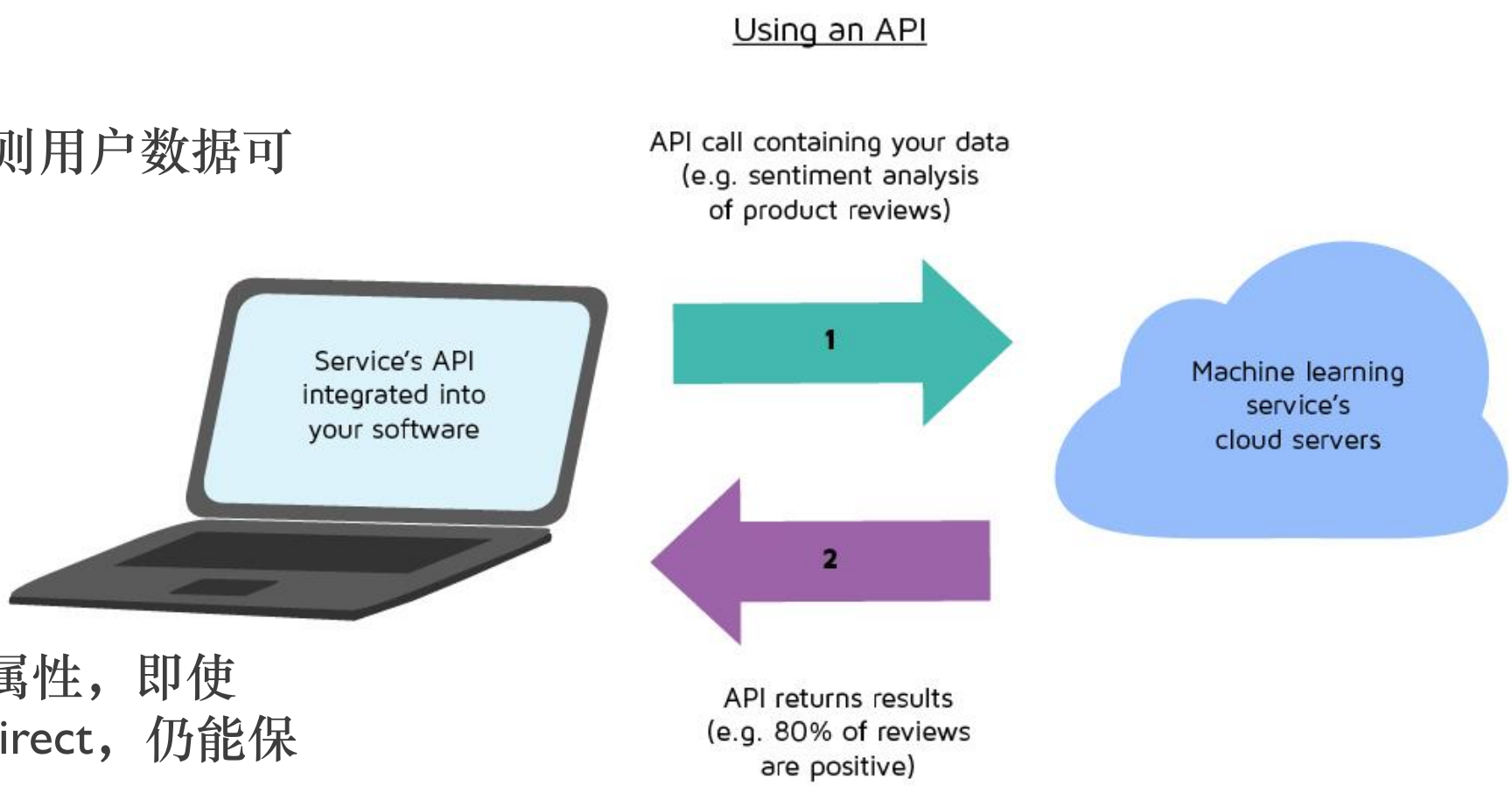
August 15–17, 2018 • Baltimore, MD, USA

ISBN 978-1-939133-04-5

SGX 的不足

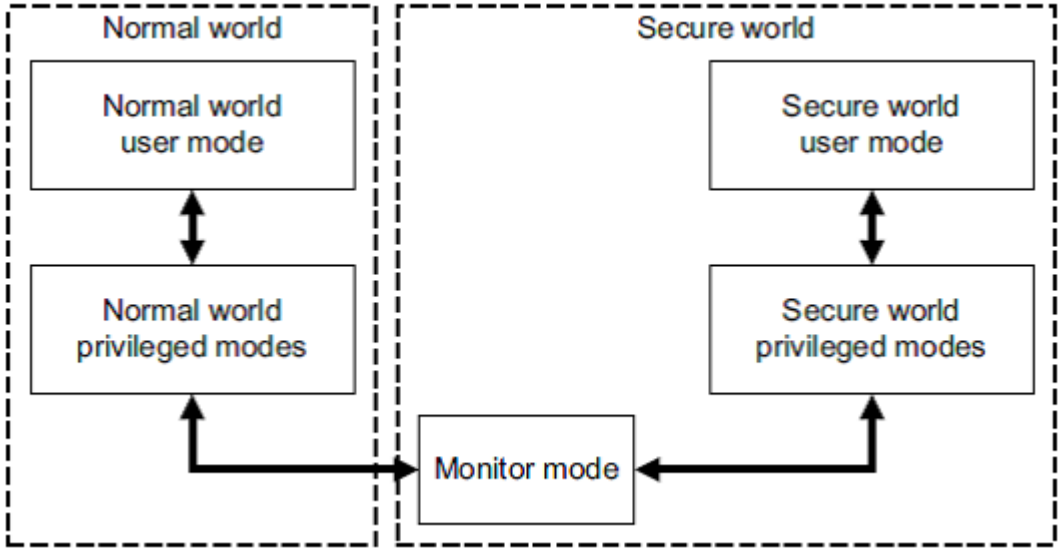
Memory Safety

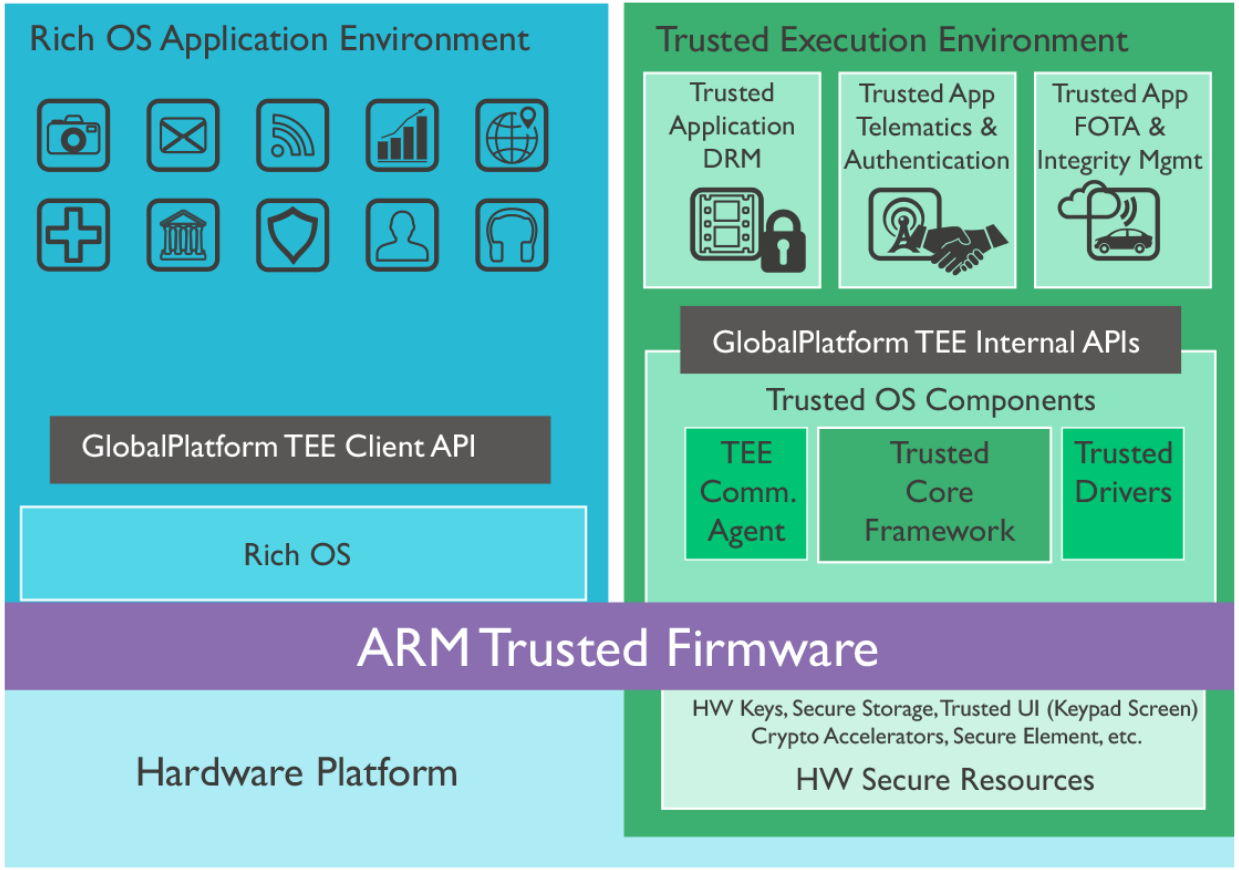
- 若代码存在漏洞，则用户数据可能被泄露



思路：代码具备某些属性，即使control flow被任意redirect，仍能保证数据不被泄露

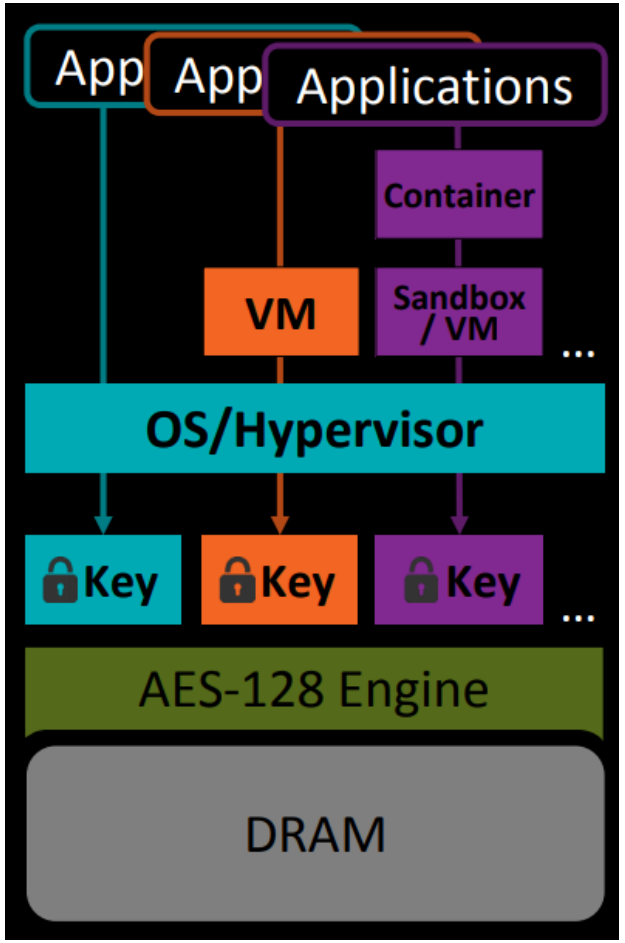
其它 TEE 技术：ARM TRUSTZONE





其它 TEE 技术：AMD SEV （SECURE ENCRYPTED VIRTUALIZATION）

- 保护虚拟机或容器 from
  - 其它虚拟机或容器
  - 系统管理员
  - Hypervisor
- Hypervisor/VM等有独立的key
- 基于加密引擎的内存隔离



其它 TEE 技术：AMD SEV （SECURE ENCRYPTED VIRTUALIZATION）

Extracting Secrets from Encrypted Virtual Machines

Mathias Morbitzer*
Fraunhofer AISEC
Garching near Munich, Ge
morbitzer@aisec.fraunho

Manuel Huber*
Fraunhofer AISEC

Julian Horsch
Fraunhofer AISEC

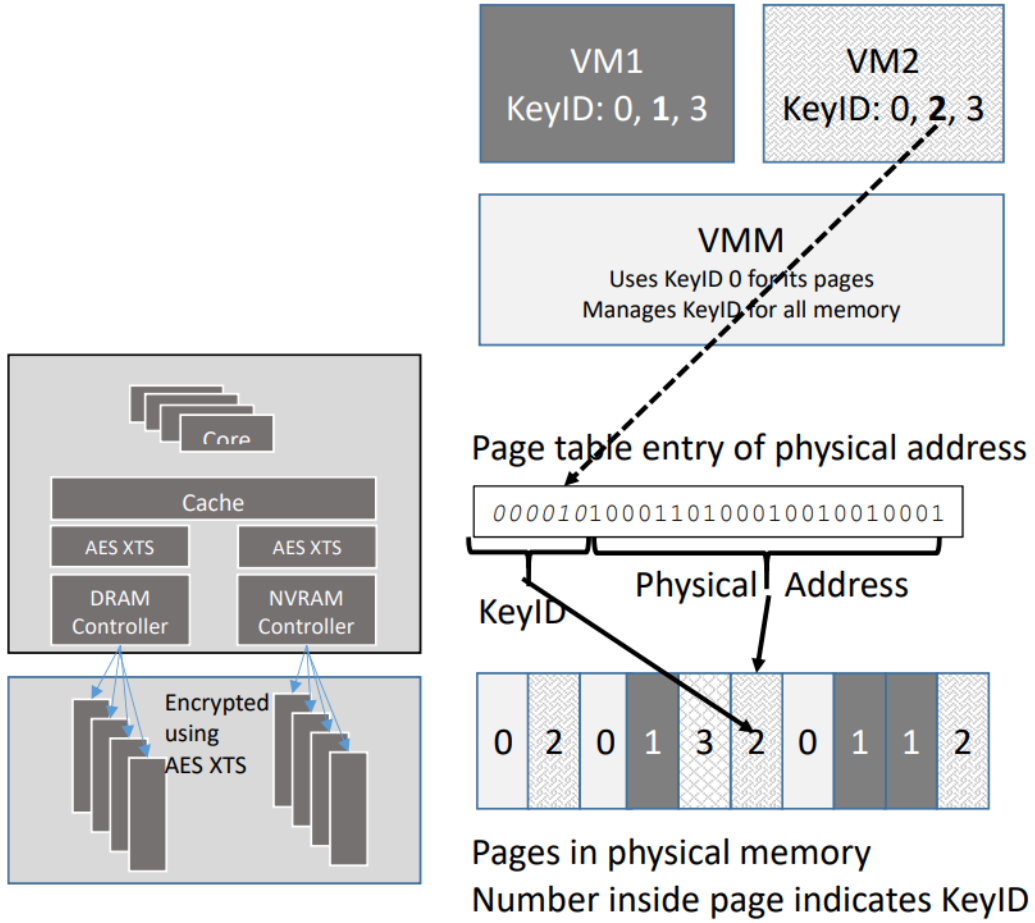
Exploiting Unprotected I/O Operations in AMD's Secure Encrypted Virtualization

Authors:
Mengyuan Li, Yinqian Zhang, and Zhiqiang Lin, *The Ohio State University;* Yan Solihin, *University of Central Florida*

SEVered: Subverting AMD's Virtual Machine Encryption

Mathias Morbitzer, Manuel Huber, Julian Horsch and Sascha Wessel
Fraunhofer AISEC
Garching near Munich, Germany
{firstname.lastname}@aisec.fraunhofer.de

其它 TEE 技术：INTEL MKTME (MULTI-KEY TOTAL MEMORY ENCRYPTION)



总结

- 硬件可信执行环境使得 practical 隐私计算成为可能
- 但目前的 TEE 仍然存在一些问题，限制了其使用场景

- 可能的解决方案
  - 软件和硬件的协同设计
  - 与密码学技术的结合

谢谢！

请批评指正！

联系方式：wangwenhao@iie.ac.cn

手机：15210983075