Exploring

AZURE CONFIDENTIAL COMPUTING

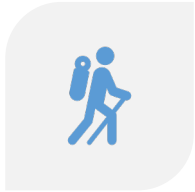
Thomas Van Laere

Microsoft Azure Consultant

Email: Thomas@thomasvanlaere.com

Twitter: @thomas_vanlaere

Blog: www.thomasvanlaere.com



MY JOURNEY

WHY

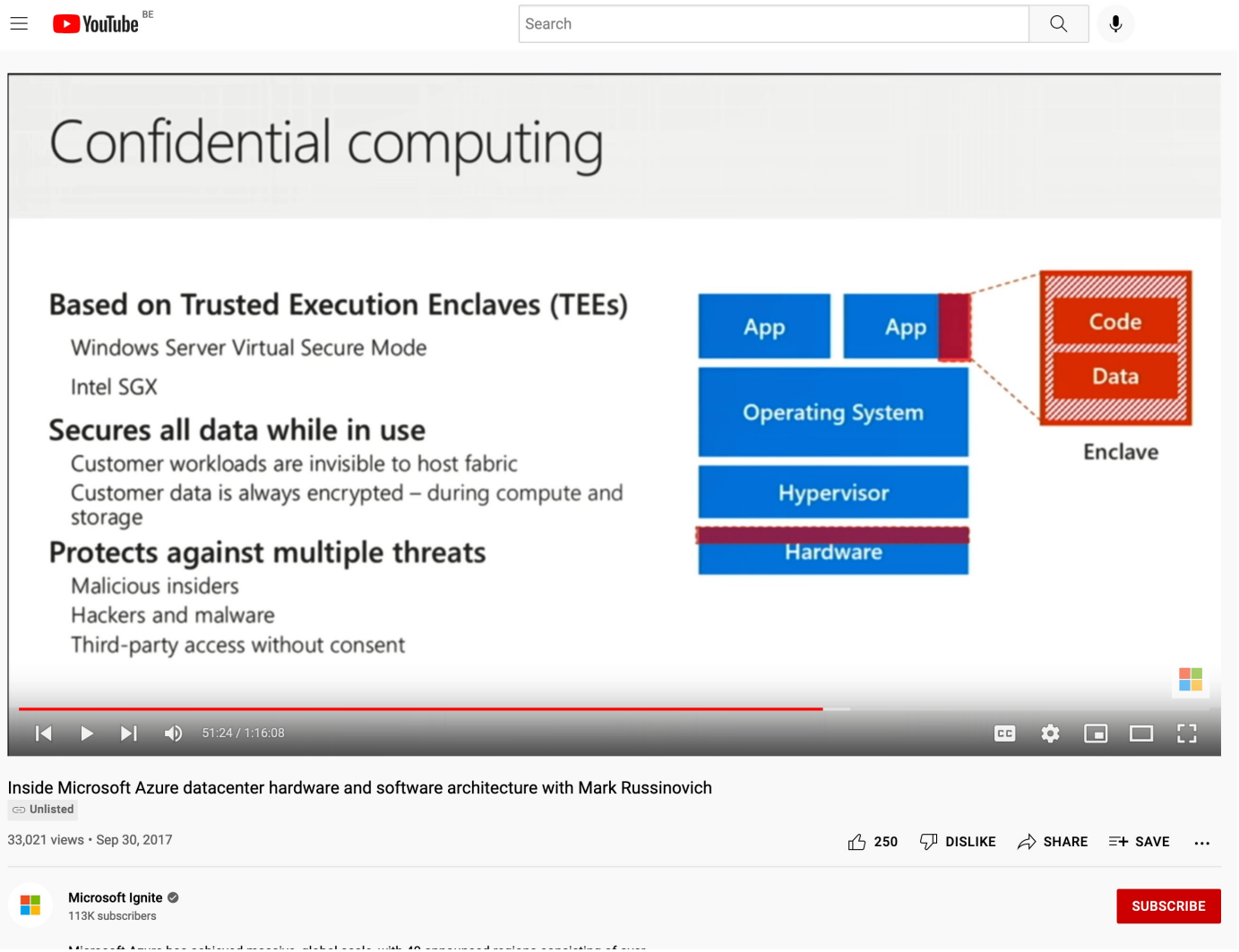
WHAT

HOW

DEMOS!

OPTIONS, SO MANY OPTIONS..

The agenda for today..



How did I get here?

Microsoft, "Inside Microsoft Azure datacenter hardware and software architecture with Mark Russinovich", September 2017, https://www.youtube.com/watch?v=Lv8fDiTNHjk

Blog / Events

Bringing confidential computing to Kubernetes

Posted on 19 November, 2019

Lachlan Evenson, Principal Program Manager - Azure Container Compute

Historically, data has been protected at rest through encryption in data stores, and in transit using network technologies, however as soon as that data is processed in the CPU of a computer it is decrypted and in plain text. New confidential computing technologies are game changing as they provide data protection, even when the code is running on the CPU, with secure hardware enclaves. Today, we are announcing that we are bringing confidential computing to Kubernetes workloads.

Confidential computing with Azure

Azure is the first major cloud platform to support confidential computing building on Intel® Software Guard Extensions (Intel SGX). Last year, we announced the preview of the DC-series of virtual machines that run on Intel® Xeon® processors and are confidential computing ready.

This confidential computing capability also provides an additional layer of protection even from potentially malicious insiders at a cloud provider, reduces the chances of data leaks and may help address some regulatory compliance needs.

Confidential computing enables several previously not possible use-cases. Customers in regulated industries can now collaborate together using sensitive partner or customers data to detect fraud scenarios without giving the other party visibility into that data. In another example customers can perform mission critical payment processing in secure enclaves.

How it works for Kubernetes

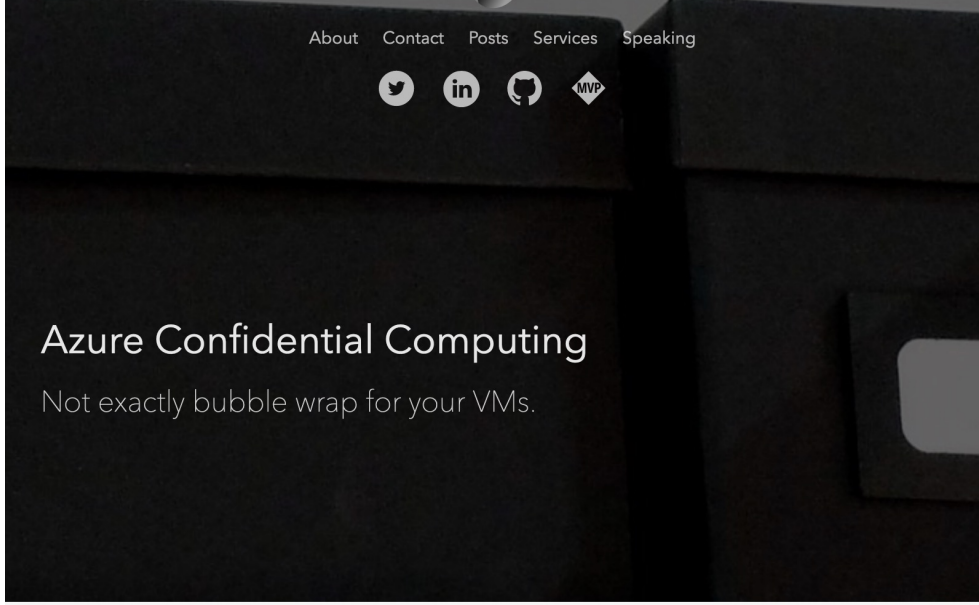
With confidential computing for Kubernetes, customers can now get this additional layer of data protection for their Kubernetes workloads with the code running on the CPU with secure hardware enclaves. Use the open enclave SDK for

How did I get here?

Lachlan Evenson, "Bringing confidential computing to Kubernetes", 19 November 2019,
https://azure.microsoft.com/en-in/blog/bringing-confidential-computing-to-kubernetes

How did I get here?

Me (lol), "Azure Confidential Computing", 17 June 2020, https://thomasvanlaere.com/posts/2020/06/azure-confidential-computing



Azure Confidential Computing

June 17, 2020

Now and again I notice that Microsoft puts out a blog post about new capabilities that have been added to the compute platform. Confidential Compute has been, somewhat, a blind spot for me. I remember first hearing about ACC when Mark Russinovich talked about it at Ignite 2017 in his "Inside Microsoft Azure datacenter hardware and software architecture" session, which is still very interesting to watch.

When I was gathering research for my previous blog post on container internals, I stumbled across an announcement about Kubernetes powered by Azure Confidential Compute. I decided to take a closer look at ACC in general and write about what I learned, to the best of my ability.

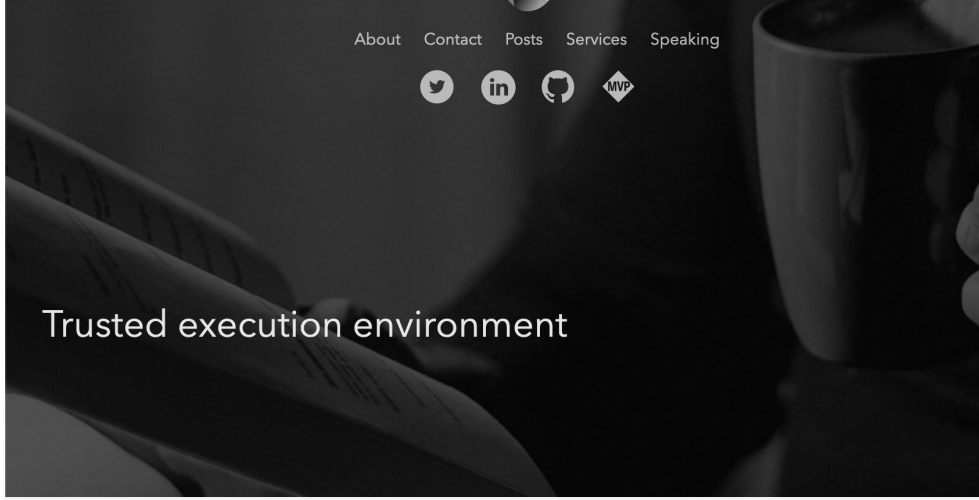
What does it take to build something using Azure Confidential compute? Without further ado let's take a look.

Why Azure Confidential Compute?

As you may know, Azure fully supports:

- End to end encryption
  - Examples of E2E encryption are HTTPS and TLS.
- At rest encryption
  - Azure Storage and SQL Server Transparent Database encryption are two common

How did I get here?



23 June 2022

Azure Confidential Computing: Confidential VMs

A closer look at AMD SEV-SNP VM SKUs.

28 April 2022

Azure Confidential Computing: IaaS

2022 edition; comes with additional bubble wrapping.

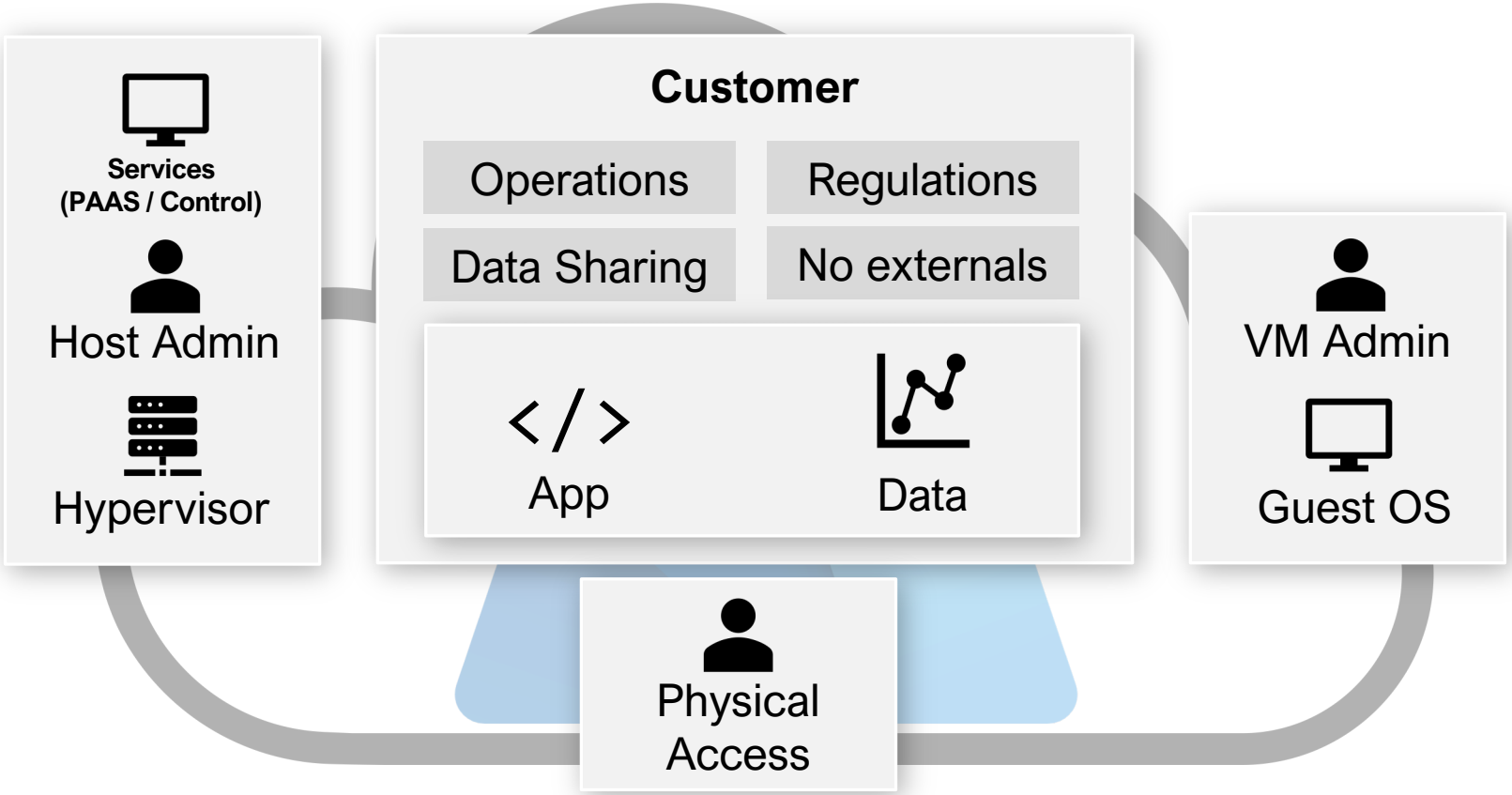
17 June 2020

Azure Confidential Computing

Not exactly bubble wrap for your VMs.

Me (lol), "Trusted Execution Environments", 23 June 2022, https://thomasvanlaere.com/tags/trusted-execution-environment/

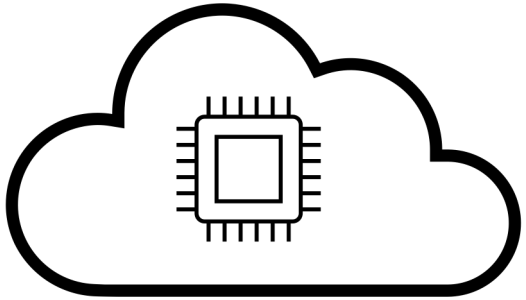
Trusting Azure today means..



Confidential Computing can help

"Azure confidential computing makes it easier to trust the cloud provider **by reducing the need for trust** across various aspects of the compute cloud infrastructure.

Azure confidential computing minimizes trust for the host OS kernel, the hypervisor, the VM admin, and the host admin."



Microsoft & contributors, "Confidential Computing on Azure", 31 August 2022, https://learn.microsoft.com/en-us/azure/confidential-computing/overview-azure-products

Privacy

Prevent unauthorized access

Compliancy

Meet regulatory compliance

Ensure

Ensure secure and untrusted collaboration

Processing

Remove liability on private data with blind processing

What drives the need to trust as little as possible?

Compliance offerings

Global
- CIS benchmark
- CSA STAR Attestation
- CSA STAR Certification
- CSA STAR self-assessment
- SOC 1
- SOC 2
- SOC 3

Global
- ISO 20000-1
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 27701
- ISO 9001
- WCAG

US government
- CJIS
- CMMC
- CNSSI 1253
- DFARS
- DoD IL2
- DoD IL4
- DoD IL5
- DoD IL6
- DoE 10 CFR Part 810
- EAR
- FedRAMP
- FIPS 140

US government
- ICD 503
- IRS 1075
- ITAR
- JSIG
- NDAA
- NIST 800-161
- NIST 800-171
- NIST 800-53
- NIST 800-63
- NIST CSF
- Section 508 VPATs
- StateRAMP

Financial services
- 23 NYCRR Part 500 (US)
- AFM and DNB (Netherlands)
- AMF and ACPR (France)
- APRA (Australia)
- CFTC 1.31 (US)
- EBA (EU)
- FCA and PRA (UK)
- FFIEC (US)
- FINMA (Switzerland)

Financial services
- FINRA 4511 (US)
- FISC (Japan)
- FSA (Denmark)
- GLBA (US)
- KNF (Poland)
- MAS and ABS (Singapore)
- NBB and FSMA (Belgium)
- OSFI (Canada)

Financial services
- OSPAR (Singapore)
- PCI 3DS
- PCI DSS
- RBI and IRDAI (India)
- SEC 17a-4 (US)
- SEC Regulation SCI (US)
- SOX (US)
- TruSight

Healthcare and life sciences
- ASIP HDS (France)
- EPCS (US)
- GxP (FDA 21 CFR Part 11)
- HIPAA (US)
- HITRUST
- MARS-E (US)
- NEN 7510 (Netherlands)

Automotive, education, energy, media, and telecommunication
- CDSA
- DPP (UK)
- FACT (UK)
- FERPA (US)
- MPA
- GSMA
- NERC (US)
- TISAX

Regional - Americas
- Argentina PDPA
- Canada privacy laws
- Canada Protected B
- US CCPA

Regional - Asia Pacific
- Australia IRAP
- China GB 18030
- China DJCP (MLPS)
- China TCS
- India MeitY
- Japan CS Gold Mark
- Japan ISMAP
- Japan My Number Act
- Korea K-ISMS
- New Zealand ISPC
- Singapore MTCS

Regional - EMEA
- EU Cloud CoC
- EU EN 301 549
- ENISA IAF
- EU GDPR
- EU Model Clauses
- Germany C5
- Germany IT-Grundschutz workbook
- Netherlands BIR 2012
- Qatar NIA

Regional - EMEA
- Russia personal data law
- Spain ENS High
- Spain LOPD
- UAE DESC
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF

https://learn.microsoft.com/en-us/compliance/regulatory/offering-home

Technical – Prevalent security model

Data at rest

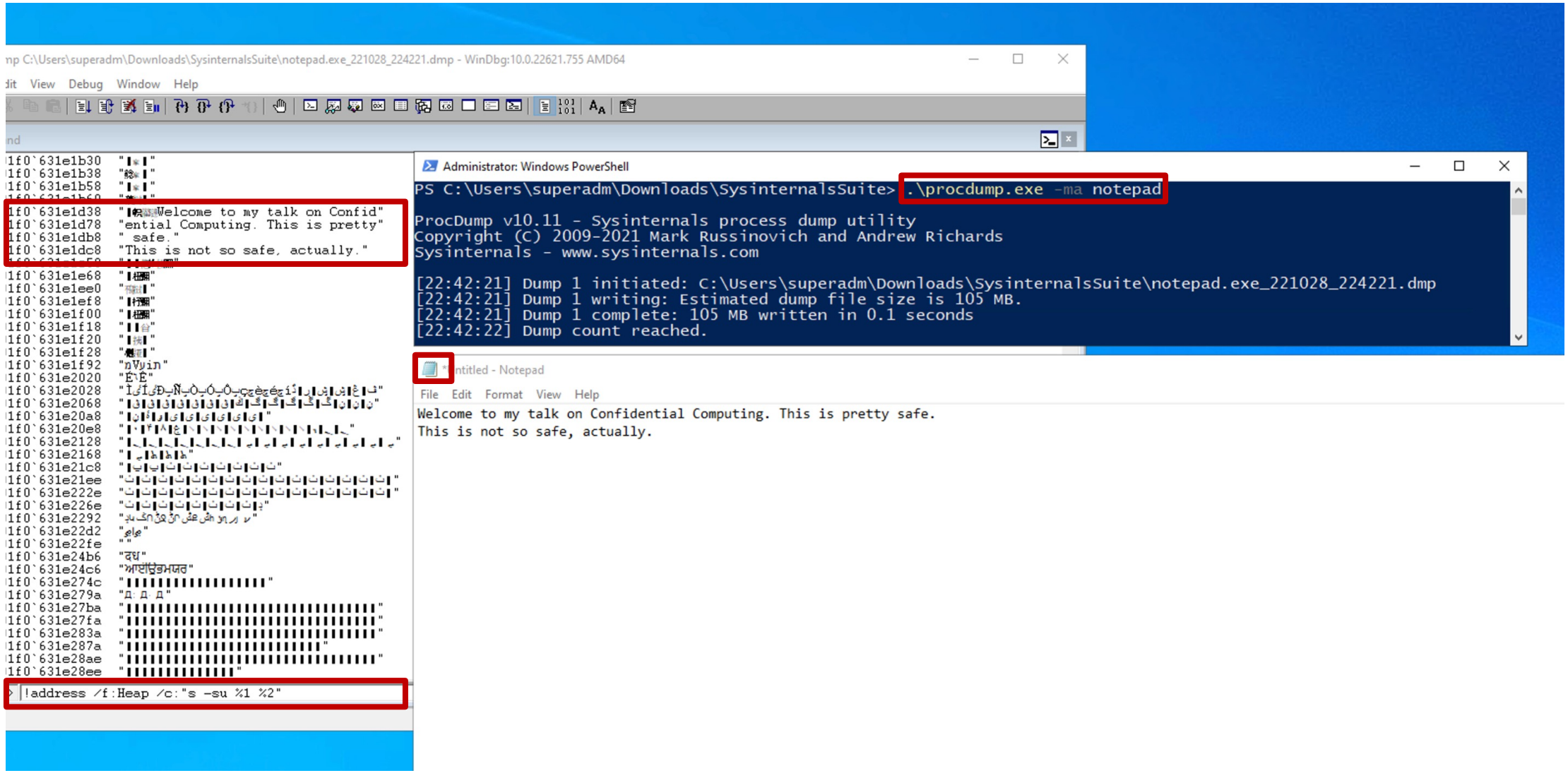
Data in transit

Data in use

Technical – Holistic security model

Existing Encryption		Confidential Computing
 Data at rest	 Data in transit	 Data in use
Ecrypted data when stored in a blob storage, database, etc..	Encrypt data as it transitions between public and private networks.	Encrypt data in RAM and during computation.

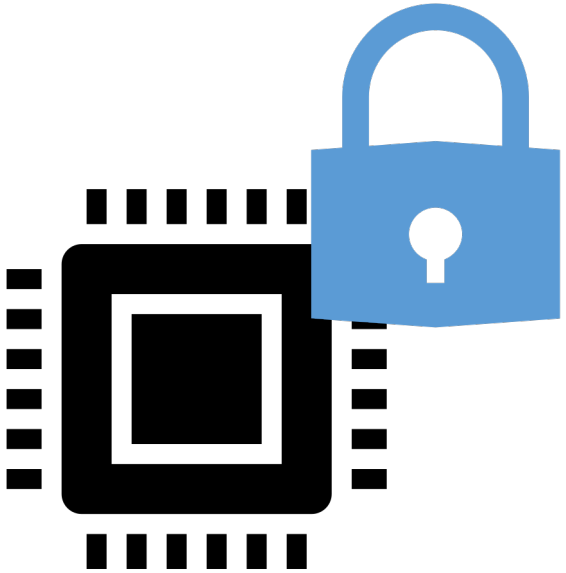
Protect against		
Malicious	**Hackers**	**Third parties**
Priviledged admins or insiders	Exploits in Hypervisor/OS	Data access without consent


np C:\Users\superadm\Downloads\SysinternalsSuite\notepad.exe_221028_224221.dmp - WinDbg:10.0.22621.755 AMD64
dit View Debug Window Help
1f0`631e1d38 "Welcome to my talk on Confid"
1f0`631e1d78 "ential Computing. This is pretty"
1f0`631e1db8 " safe."
1f0`631e1dc8 "This is not so safe, actually."
!address /f:Heap /c:"s -su %1 %2"
Administrator: Windows PowerShell
PS C:\Users\superadm\Downloads\SysinternalsSuite> .\procdump.exe -ma notepad
ProcDump v10.11 - Sysinternals process dump utility
Copyright (C) 2009-2021 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
[22:42:21] Dump 1 initiated: C:\Users\superadm\Downloads\SysinternalsSuite\notepad.exe_221028_224221.dmp
[22:42:21] Dump 1 writing: Estimated dump file size is 105 MB.
[22:42:21] Dump 1 complete: 105 MB written in 0.1 seconds
[22:42:22] Dump count reached.
ntitled - Notepad
File Edit Format View Help
Welcome to my talk on Confidential Computing. This is pretty safe.
This is not so safe, actually.

Enables new scenarios

Defensive	Protection	Sharing
Defense from others	Protect customer data from myself and Azure	Securely share data with multi-party
Malicious admins	Guest/Host OS kernel	Multi-Party Computation
Hackers	VM/Host admin	Multi-Party Analytics
Access without consent	Hypervisor or hardware access	Federated Learning

Public cloud
with
private data center assurances



Protecting - Data in use

Privacy-Preserving Computation

- Homomorphic Encryption

Trusted Execution Environments

- Hardware TEEs

Overview | Release news | People | Publications | Videos | News & features

Microsoft SEAL—powered by open-source homomorphic encryption technology—provides a set of encryption libraries that allow computations to be performed directly on encrypted data. This enables software engineers to build end-to-end encrypted data storage and computation services where the customer never needs to share their key with the service.

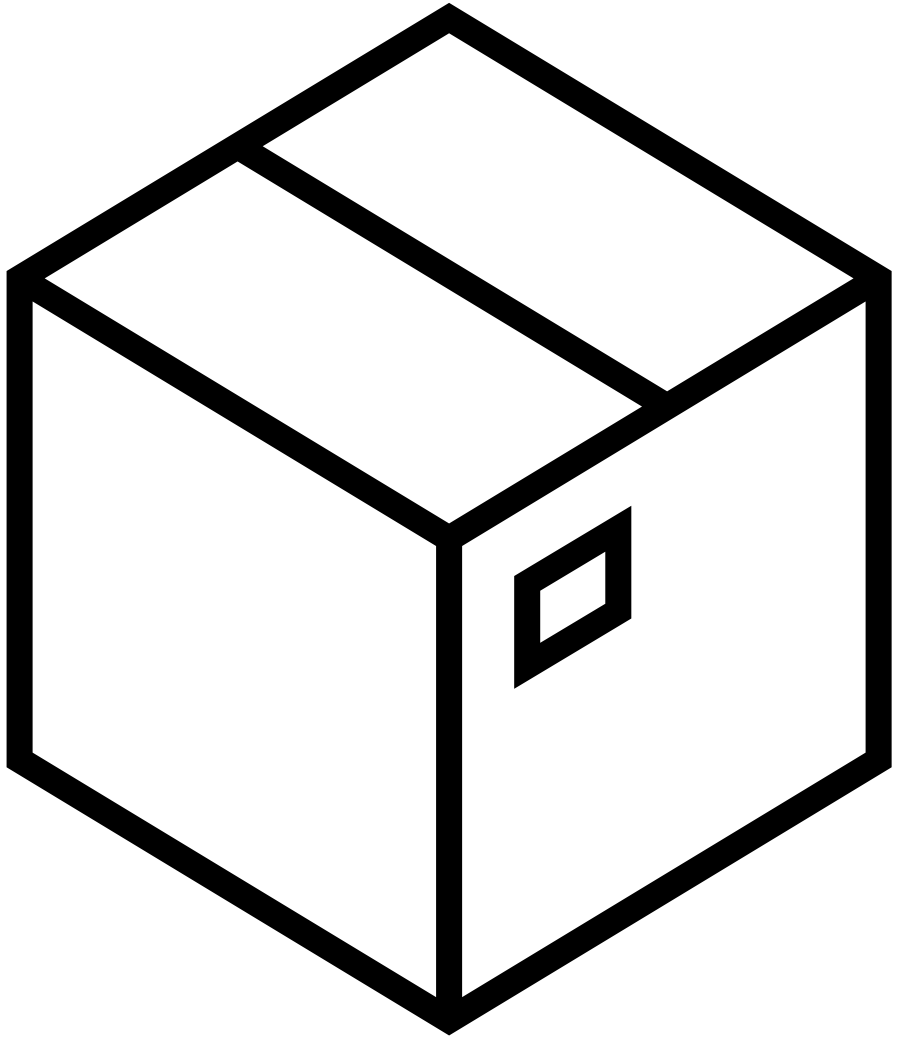
Microsoft SEAL is open source (MIT license). Start using it today!

Download

https://github.com/Microsoft/SEAL

Trusted Execution Environments (TEE)

By executing computations inside of a **hardware-based** TEE, we can prevent unauthorized access or modification of applications and data while they are in use.



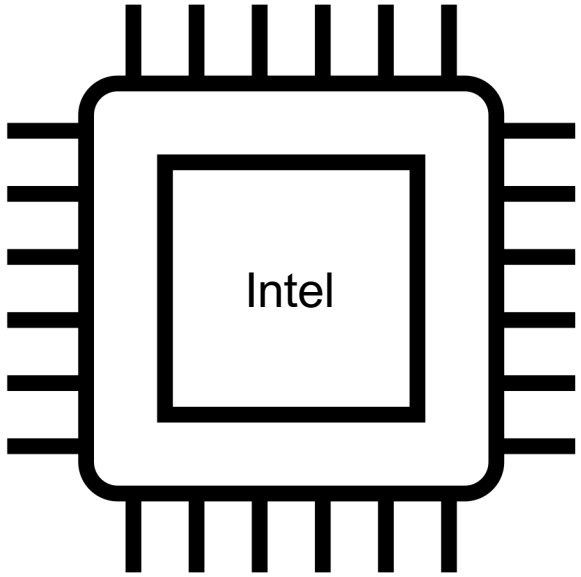
Why is hardware necessary for Confidential Computing

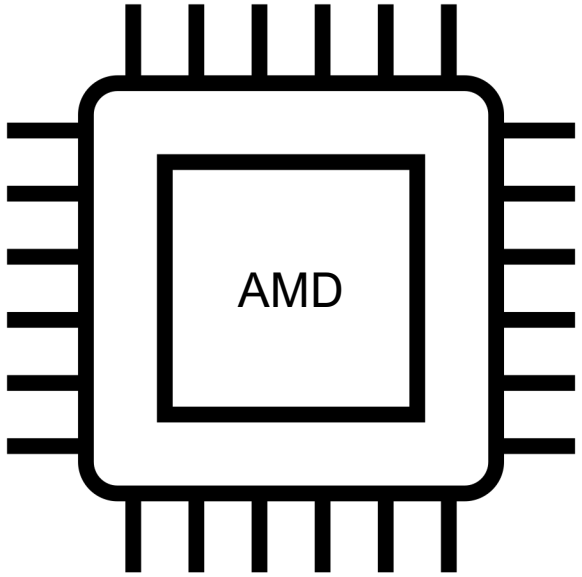
“Security is only as strong as the layers below it, since security in any layer of the compute stack could potentially be circumvented by a breach at an underlying layer.

This drives the need for security solutions at the lowest layers possible, down to the silicon components of the hardware.

By providing security though the lowest layers of hardware, with a minimum of dependencies, it is possible to remove the operating system and device driver vendors, platform and peripheral vendors, and service providers and their admins, from the list of required trusted parties, thereby reducing exposure to potential compromise at any point in the system lifecycle.”

Confidential Computing Consortium, "A Technical Analysis of Confidential Computing”, October 2021
https://confidentialcomputing.io/wp-content/uploads/sites/85/2022/11/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.2_updated_2022-11-02.pdf





A tale of two CPU vendors

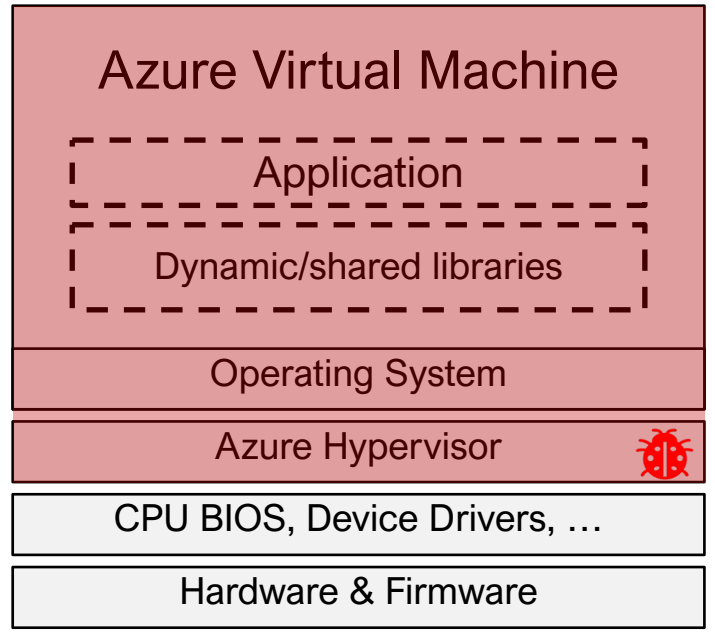
Trusted Computing Base

"The trusted computing base (TCB) refers to all of a system's hardware, firmware, and software components that provide a secure environment.

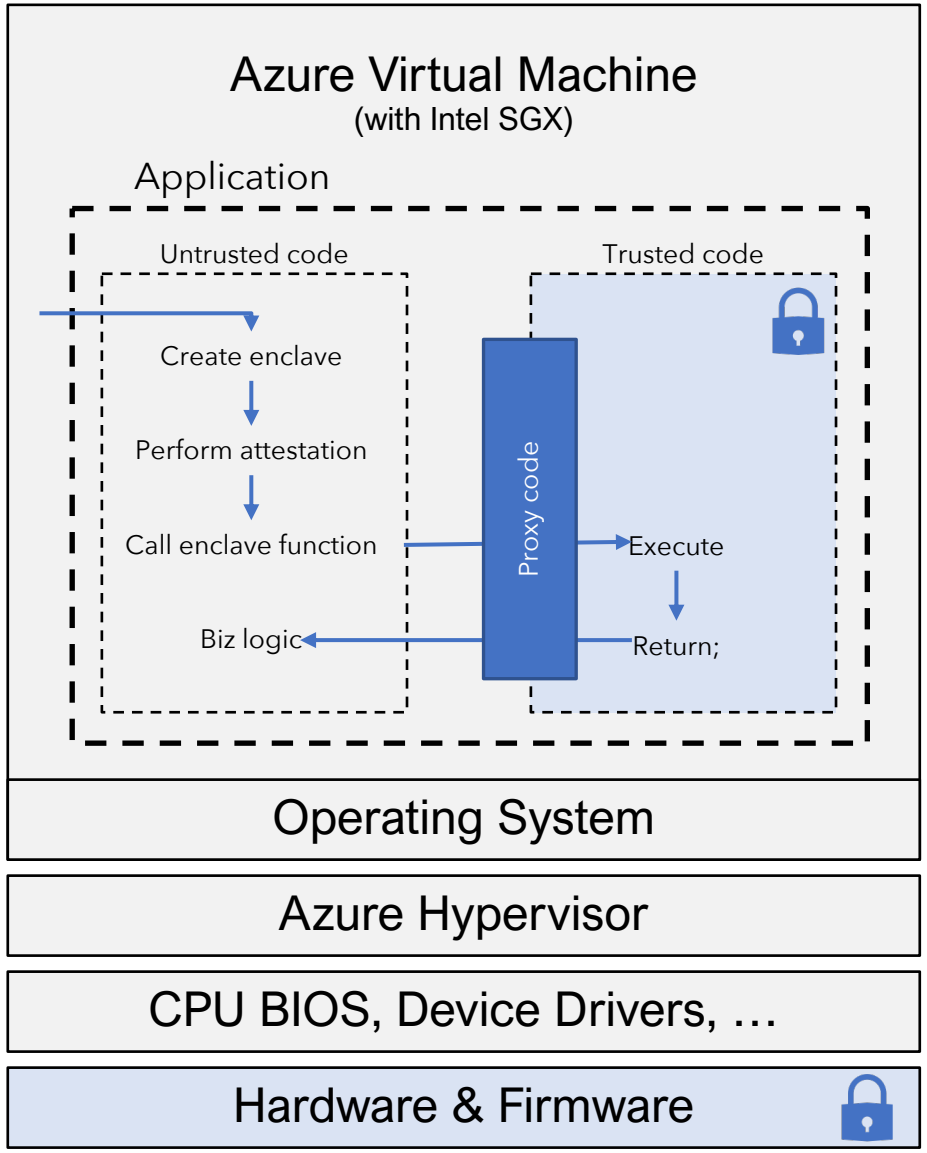
*The components inside the TCB are considered "**critical**".*

*If **one** component inside the TCB is **compromised**, the **entire system**'s security may be **jeopardized**.*

*A **lower TCB** means **higher security**."*



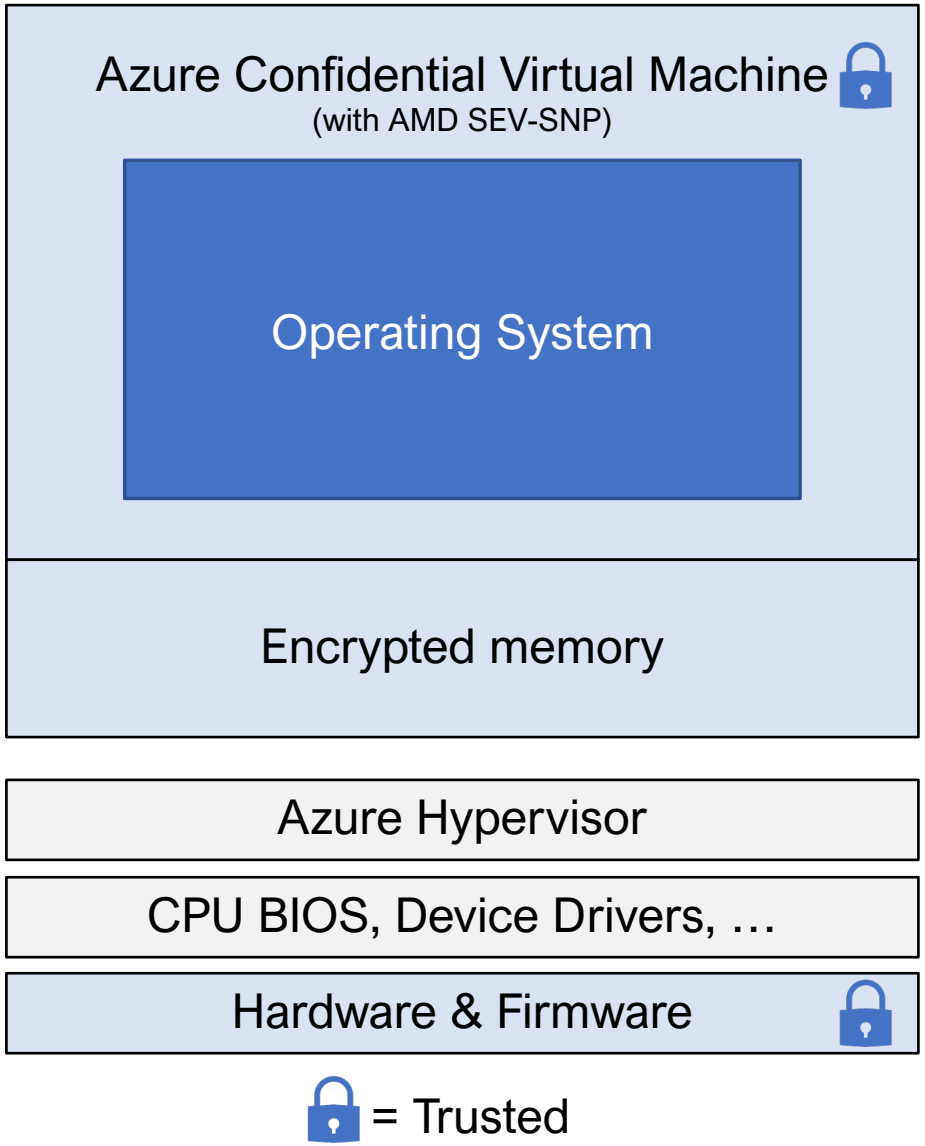
Microsoft & contributors, "What is confidential computing?", 23 Augusts 2022, https://learn.microsoft.com/en-us/azure/confidential-computing/overview



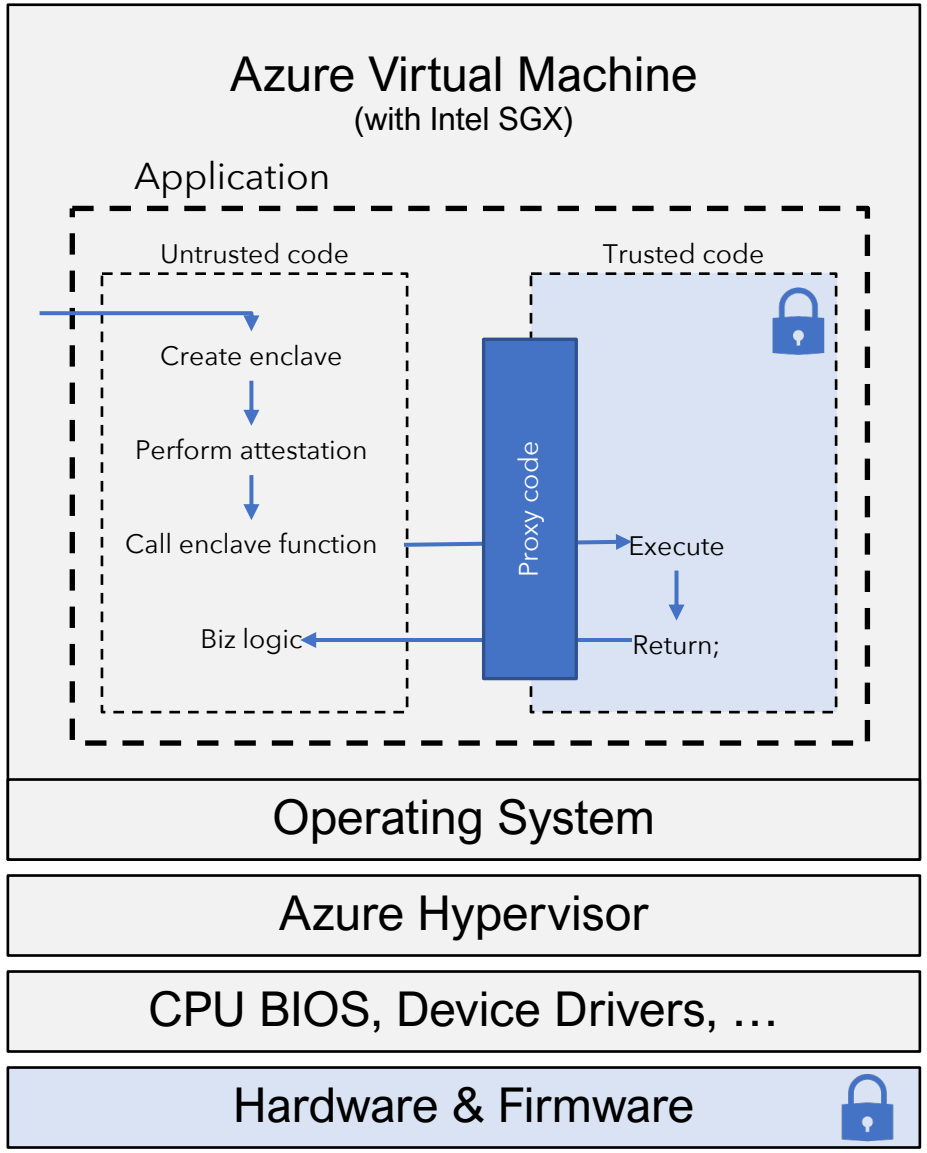
VMs with App Enclaves (Intel SGX)

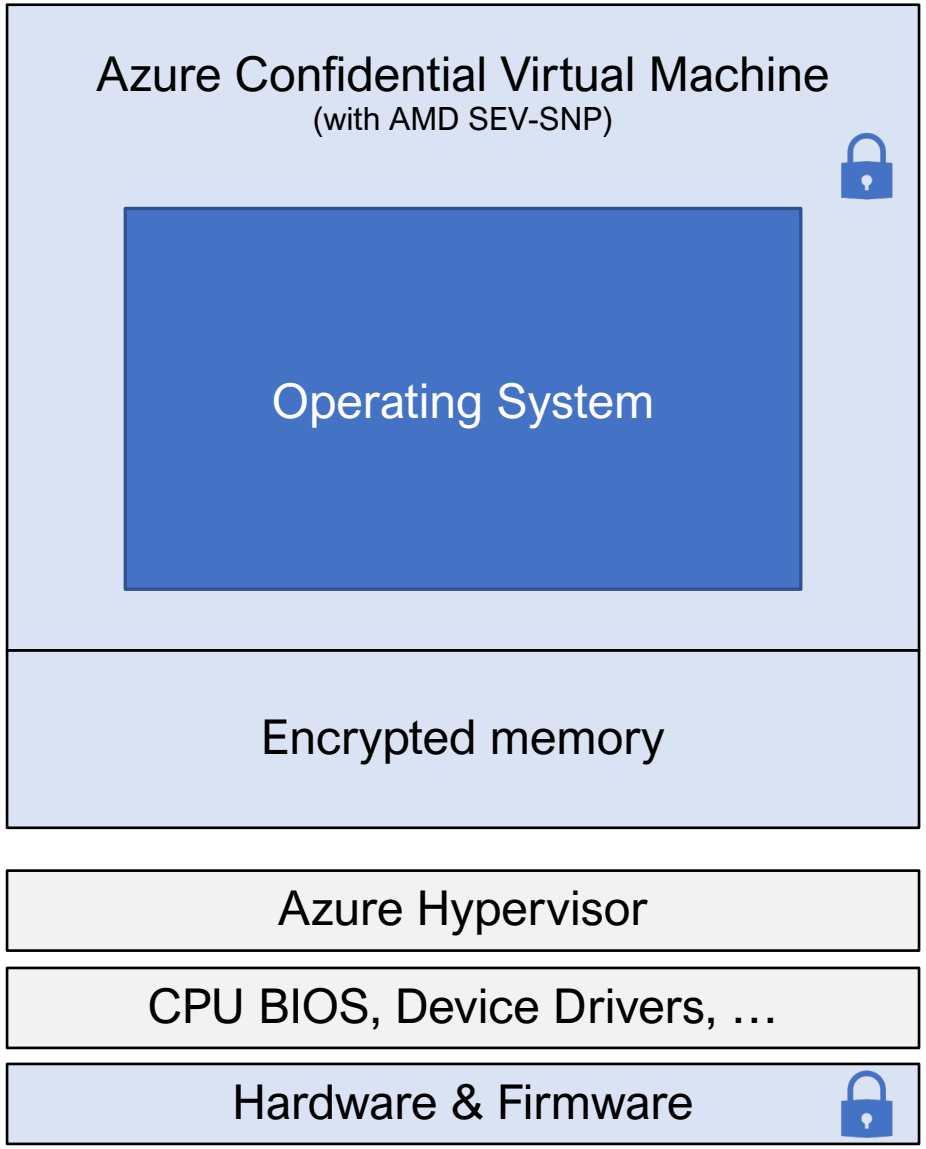
* DCsv2 (General purpose)
** DCsv3 and DCdsv3 (General purpose)

Confidential Virtual Machines (SEV-SNP)



* DCasv5 and DCadsv5 (General purpose)
** ECasv5 and ECadsv5 (Memory optimized)


Azure Virtual Machine
(with Intel SGX)
Application
Untrusted code
Trusted code
Create enclave
Perform attestation
Call enclave function
Proxy code
Execute
Biz logic
Return;
Operating System
Azure Hypervisor
CPU BIOS, Device Drivers, …
Hardware & Firmware


Azure Confidential Virtual Machine
(with AMD SEV-SNP)
Operating System
Encrypted memory
Azure Hypervisor
CPU BIOS, Device Drivers, …
Hardware & Firmware

= Trusted

Confidential Computing Spectrum

Trusted Launch

Generation 2 Azure VMs
Increased protection for
(non-)confidential VM SKUs

Confidential VMs

AMD SEV-SNP VM SKUs
"Legacy" workloads:
- Azure Virtual Machines
- AKS Node Pools
- Azure Virtual Desktop
- SQL Server

NVIDIA NCC VM SKUs*
Leverage GPUs for AI/ML workloads

Confidential Containers

Azure Container Instances*
Lift-and-shift containers using
AMD SEV-SNP backed container groups

Intel SGX OSS || Partner solutions
Lift-and-shift container images
inside SGX enclave

Enclave aware containers
Lift-and-shift existing SGX workloads
to run inside of a container

Enclave-aware apps

OpenEnclave SDK
Hardware-based TEE w/ SGX in C/C++

Confidential Consortium Framework
Enables multi-party compute

EGo SDK
Enables confidential Go apps

PAAS offerings

Azure Key Vault Managed HSM
Azure Attestation
Azure SQL Always Encrypted Secure Enclaves
Azure Confidential Ledger
Etc..

EASIER TO ONBOARD LEGACY APPS

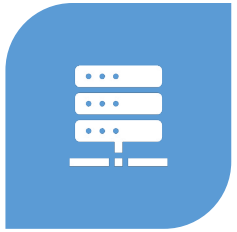
LARGER TCB

CUSTOM SOLUTIONS

GRANULAR SECURITY CONTROL

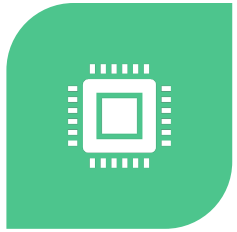
*** Preview**

TEEs – supporting actors



HARDWARE ROOT OF TRUST

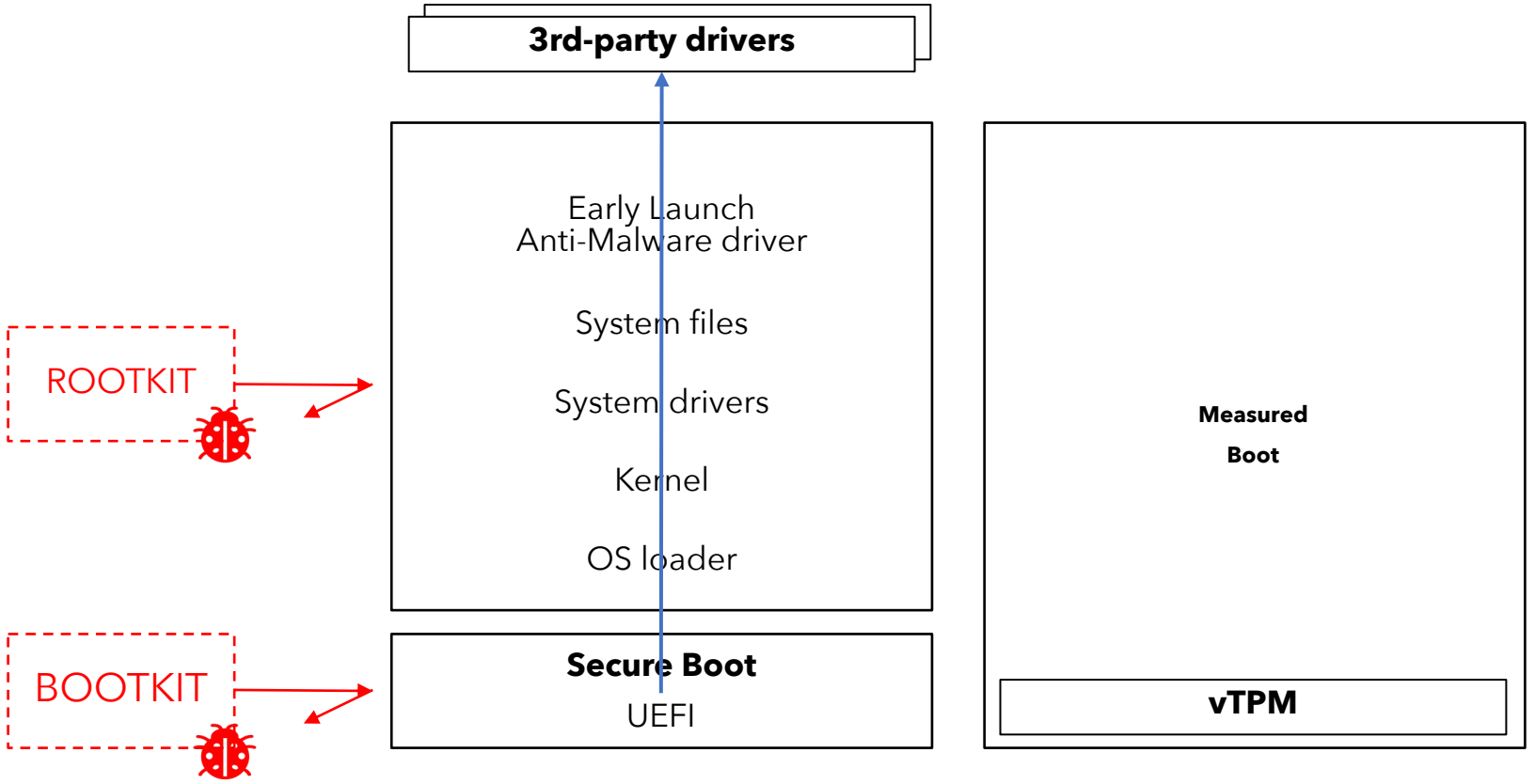
REMOTE ATTESTATION



MEMORY ISOLATION AND ENCRYPTION

SECURE KEY MANAGEMENT

TRUSTED LAUNCH



Trusted Launch

Trusted Launch Demo


Confidential VM Demo

SGX Enclaves demo

New scenarios


Internal Tools


SaaS offerings


ISV Partners


Finance


Governments


Healthcare

Dev tools


VS Studio/Code


WinDbg


CCF SDK


OpenEnclave SDK


Mystikos


Containerization


Azure Data Share

Confidential Enabled Azure PAAS


Azure SQL


Azure Machine Learning


Azure Key Vault


Azure Confidential Ledger


Azure Attestation


Azure Kubernetes Service


Azure IoT

Cloud and Edge


Azure VMs w/ App Enclaves


Azure Confidential VMs


Azure Trusted Launch


Azure IoT Edge Devices


Confidential Containers on ACI**


Azure Virtual Desktop with CVMs*


Azure Managed CCF**

New Hardware


Intel


AMD


ARM


NVIDIA**

Standardization

Confidential Computing Consortium

Microsoft Research

Public preview
****Limited preview***

Confidential Computing at Microsoft

Cornell University

arXiv > cs > arXiv:2108.04575

Computer Science > Cryptography and Security

[Submitted on 10 Aug 2021 (v1), last revised 26 Aug 2021 (this version, v4)]

One Glitch to Rule Them All: Fault Injection Attacks Against AMD's Secure Encrypted Virtualization

Robert Buhren, Hans Niklas Jacob, Thilo Krachenfels, Jean-Pierre Seifert

AMD Secure Encrypted Virtualization (SEV) offers protection mechanisms for virtual machines in untrusted environments through memory and register encryption. To separate security-sensitive operations from software executing on the main x86 cores, SEV leverages the AMD Secure Processor (AMD-SP). This paper introduces a new approach to attack SEV-protected virtual machines (VMs) by targeting the AMD-SP. We present a voltage glitching attack that allows an attacker to execute custom payloads on the AMD-SPs of all microarchitectures that support SEV currently on the market (Zen 1, Zen 2, and Zen 3). The presented methods allow us to deploy a custom SEV firmware on the AMD-SP, which enables an adversary to decrypt a VM's memory. Furthermore, using our approach, we can extract endorsement keys of SEV-enabled CPUs, which allows us to fake attestation reports or to pose as a valid target for VM migration without requiring physical access to the target host. Moreover, we reverse-engineered the Versioned Chip Endorsement Key (VCEK) mechanism introduced with SEV Secure Nested Paging (SEV-SNP). The VCEK binds the endorsement keys to the firmware version of TCB components relevant for SEV. Building on the ability to extract the endorsement keys, we show how to derive valid VCEKs for arbitrary firmware versions. With our findings, we prove that SEV cannot adequately protect confidential data in cloud environments from insider attackers, such as rogue administrators, on currently available CPUs.

Subjects: **Cryptography and Security (cs.CR)**
Cite as: arXiv:2108.04575 **[cs.CR]**
(or arXiv:2108.04575v4 **[cs.CR]** for this version)
https://doi.org/10.48550/arXiv.2108.04575

Submission history

From: Robert Buhren [view email]
[v1] Tue, 10 Aug 2021 10:47:47 UTC (421 KB)
[v2] Wed, 11 Aug 2021 10:55:23 UTC (420 KB)
[v3] Thu, 12 Aug 2021 13:54:27 UTC (420 KB)
[v4] Thu, 26 Aug 2021 13:08:55 UTC (434 KB)

be-all and end-all?

Summary

- Private DC guarantees, in the cloud
- Different trust levels for new scenarios
- Trusted Launch available for all VM SKUs
- Lift-and-shift with Confidential VMs
- Jumpstart SGX enclave development with partner/OSS enablers
- Cost efficient

Want to learn more?

Azure Confidential Computing

- https://aka.ms/ConfidentialCompute

Confidential containers with Partner or Open-Source Software enablers

- https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-containers-enclaves

What is Guest Attestation for Confidential VMs?

- https://learn.microsoft.com/en-us/azure/confidential-computing/guest-attestation-confidential-vms

Confidential Computing Consortium

- https://confidentialcomputing.io/

AZURE CONFIDENTIAL COMPUTING: IAAS (2022)

AZURE CONFIDENTIAL COMPUTING: CONFIDENTIAL VMS (2022)

AZURE CONFIDENTIAL COMPUTING (2020) (SGX/OPENENCLAVE)

Want to learn more?
https://thomasvanlaere.com

Thank you!