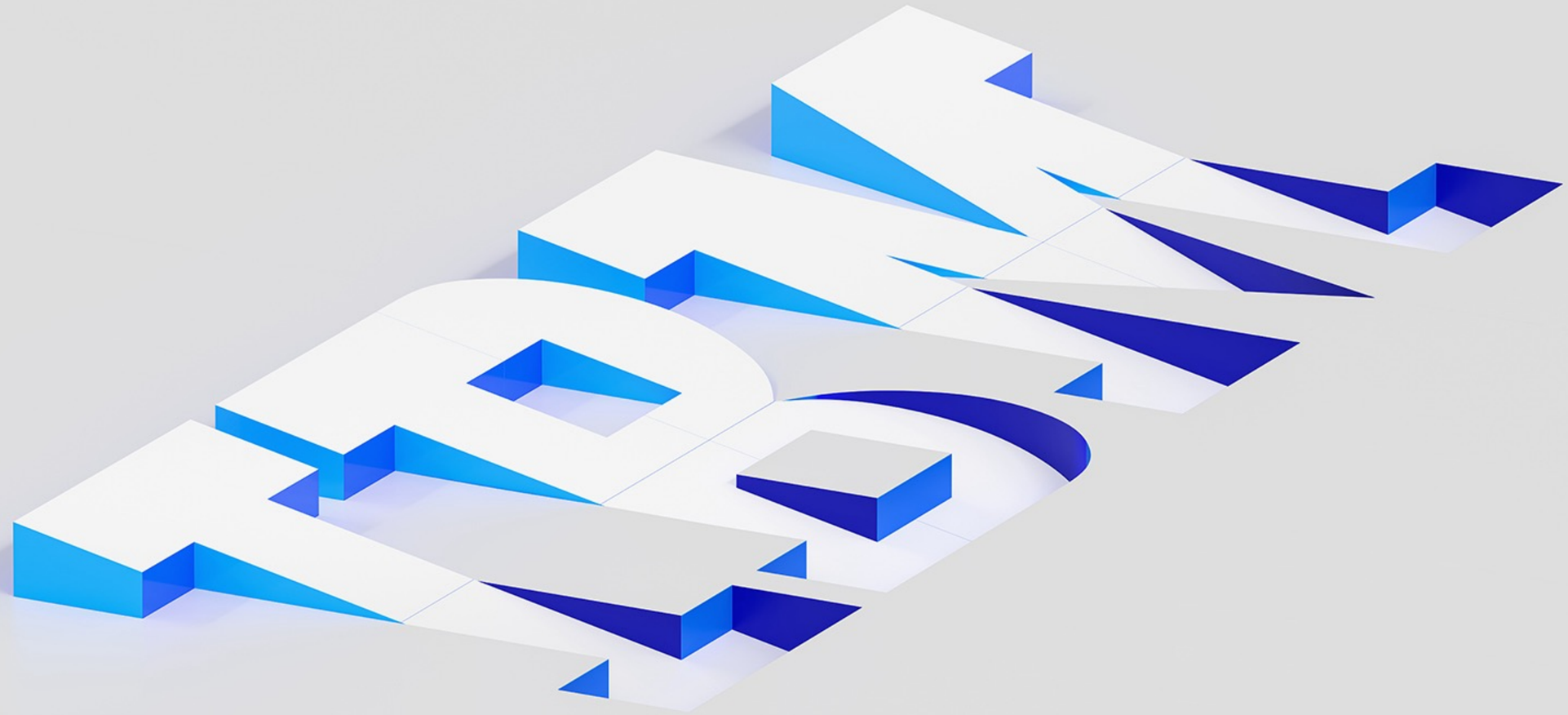


Confidential Computing on IBM Z and LinuxONE with Hyper Protect Virtual Servers 2.1.x Wildfire Workshop – December 12, 2023

Barry Silliman
Consulting IT Specialist
silliman@us.ibm.com
240.674.7222

Garrett Woodworth
Senior IT Specialist
garrett.lee.woodworth@ibm.com
510.600.5652

IBM

Agenda

Definition of confidential computing

IBM Z and LinuxONE and confidential computing

Hyper Protect Virtual Servers 2.1.x overview

Additional resources

Lab overview

Confidential Computing…

What is it?

“The protection of data in use through a hardware-based technique”

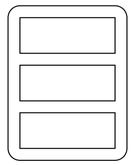
Trusted Execution Environment (TEE) = hardware-based secure enclave where memory (data in use) is protected

- Confidential Computing Consortium

Trusted Execution Environment (TEE)

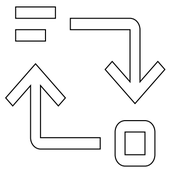
Confidential computing completes the triad of data protection

PREVALENT PROTECTIONS | INCREASING FOCUS



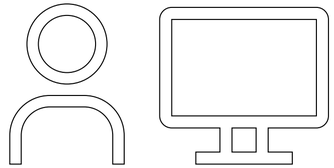
Data at rest

Inactive data that is not currently being accessed or transferred



Data in transit

Traveling between public or private networks



Data in use

Actively being accessed by an application or a user and stored in memory

CONFIDENTIAL COMPUTING

IBM Z’s and LinuxONE’s first implementation of Confidential Computing: Secure Service Container LPAR

IBM Secure Service Container

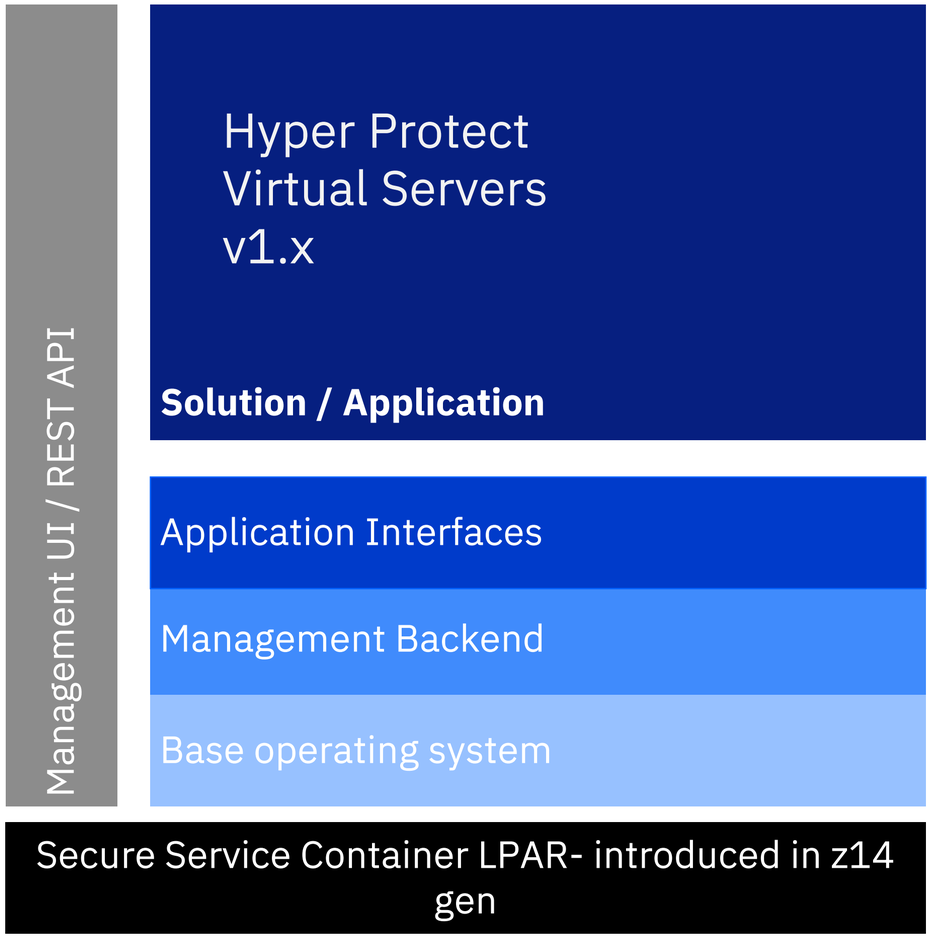
Provides the base infrastructure for an integration of operating system, middleware, and software components. It provides the key security capabilities for Hyper Protect Services, both in the public cloud and on-premises

Secure Service Container

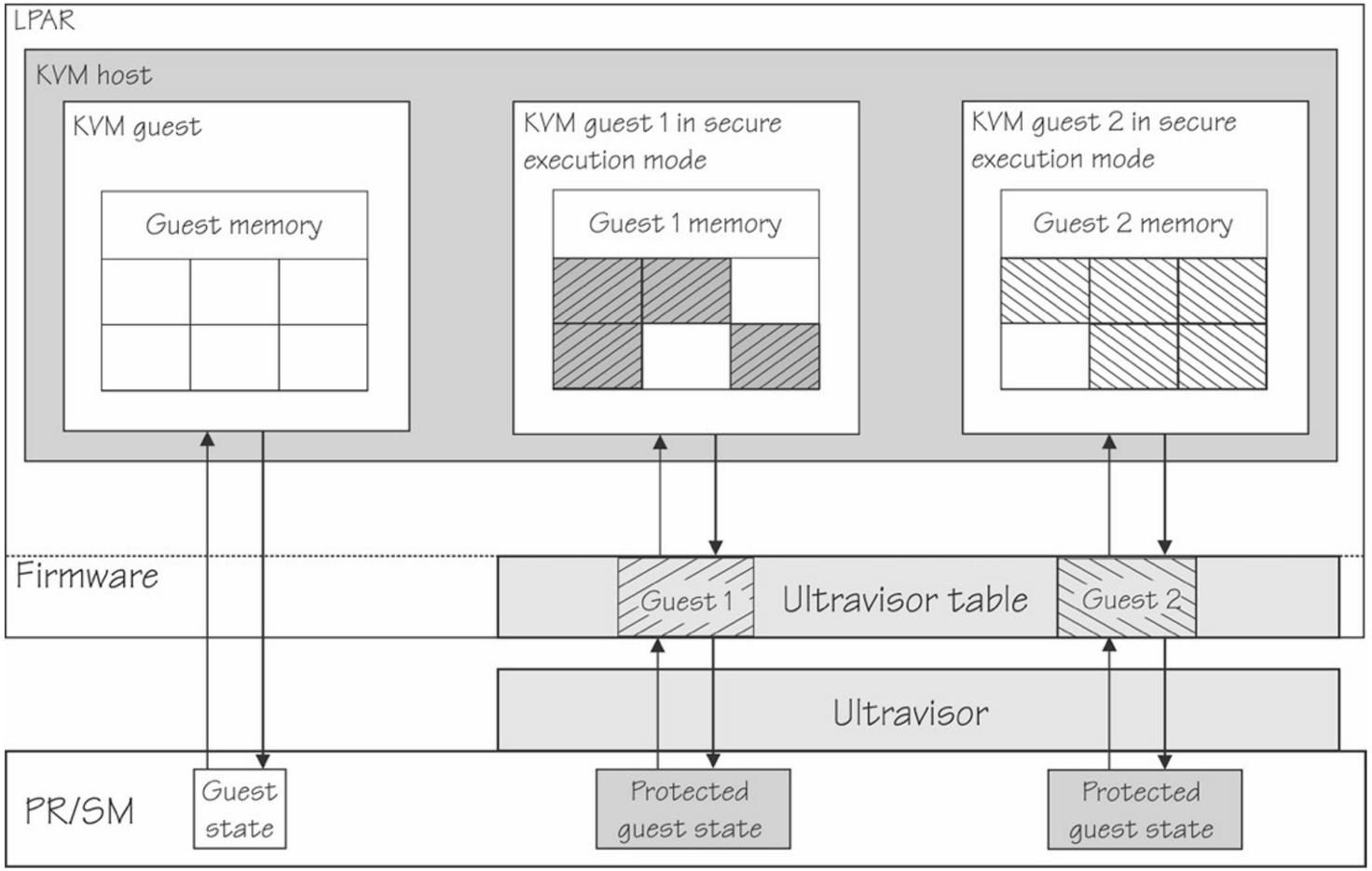
Secure Boot
- Only boots authorized workloads

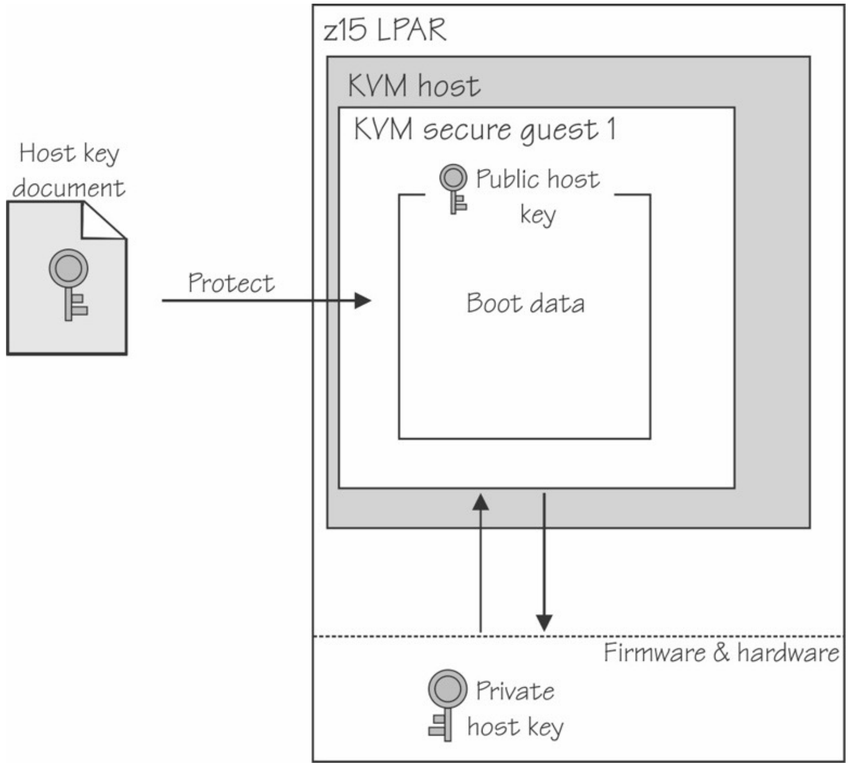
Data Encryption
- All data and code in flight and at rest
- Debug data i.e., dumps, diagnostic log files

Restricted Access
- Encrypted communication via REST APIs
- No direct operating system level access
- No infrastructure administrator access to memory or processor state



IBM Z's and LinuxONE's newest implementation of Confidential Computing: Secure Execution for Linux



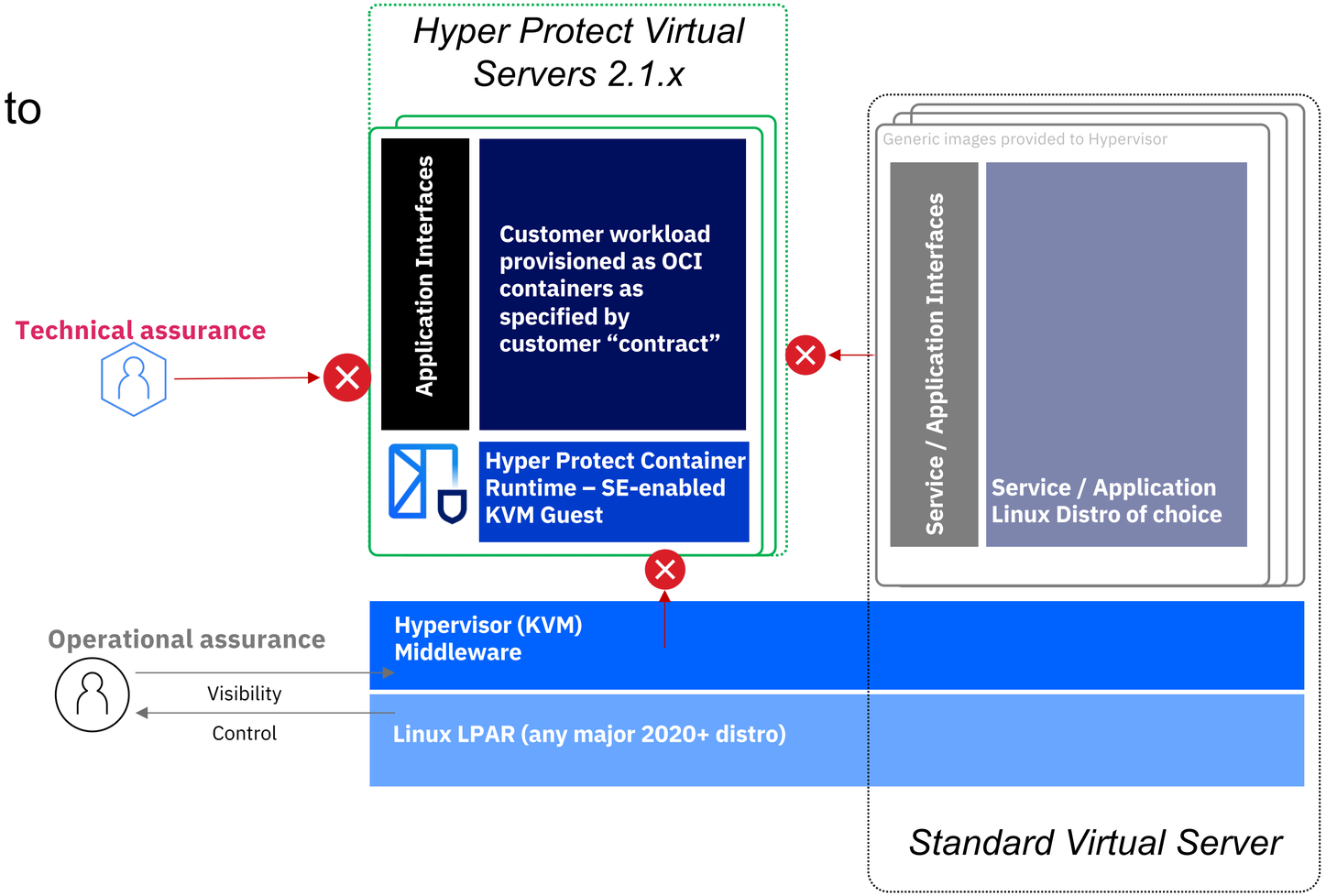


No hardware administrator, no KVM code, and no KVM administrator can access the data in a guest that was started as an IBM Secure Execution guest. Read more here: https://www.ibm.com/docs/en/linux-on-systems?topic=virtualization-secure-execution

Hyper Protect Virtual Servers 2.1.x is based on Secure Execution for Linux

Hyper Protect Virtual Servers 2.1.x takes advantage of Secure Execution technology to provide a secure boundary around each instance

- Isolation from the OS and Hypervisor vulnerabilities
- Isolation between instances
- Technical assurance that host administrator cannot access the environment



Reduce common attack vectors with Hyper Protect Virtual Servers

Remote Attack

- **No** interactive access (SSH) into protected Trusted Execution Environment

Privilege Escalation

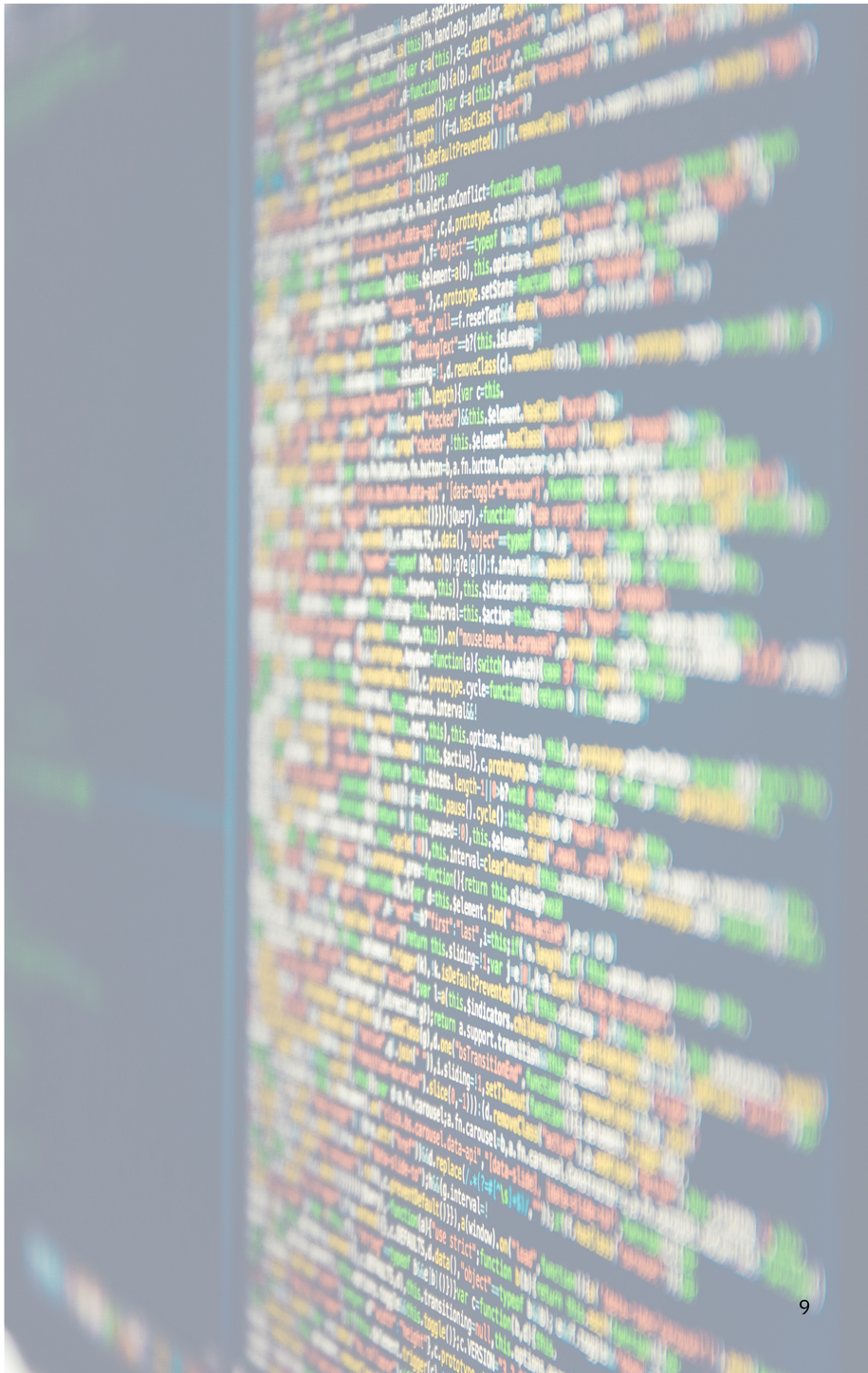
- Workload isolation against OS/Hypervisor/Middleware
- Isolation between Secure Execution Virtual Machines/Enclaves

Insider Attack

- Access to hardware does not mean data is compromised
- Only authorized workload can access customer data (confidential computing: data-in-use protected)

Image Tampering/Malware

- Encrypted image and only deployable on systems with Secure Execution
- Multi-party encrypted contract with optional attestation



Encrypted Multi-Party Contract

Enables customer to enforce Zero-Trust concepts
Individual secrets of workload, deployment and more

IBM Hyper Protect

data-in-use protection
through Secure Execution
HW-based protected keys

Workload (Provider)

(Secure) Build Pipeline

workload
(OCI image)

Workload
registry
parameter
secrets

encrypt
against IBM Hyper Protect secret

Workload
843NFEW98RU4
32INF42FZ4238HF
8H43QZV04HWK
VJ0V9347T90243

Customer or ISV provided container repository

IBM Hyper Protect Container Runtime

validate

workload
(OCI image)

deploy

Customer specific

Environment

Environment
ports
volumes
secrets

encrypt
against IBM Hyper Protect secret

Environment
A78B09312BA
493NCASAKJ
JGA8932FK3
12ENWF094L
U3IT4301G4

Attestation (Auditor specific)

encrypt
against IBM Hyper Protect secret

Attestation
public key

Attestation
7841AHABCAC

Hyper Protect Contract

Workload
843NFEW98RU4
32INF42FZ4238HF
8H43QZV04HWK
VJ0V9347T90243

Environment
A78B09312BA
493NCASAKJ
JGA8932FK3
12ENWF094L
U3IT4301G4

Attestation
7841AHABCAC

provide/deploy

decrypt

Hyper Protect Contract

Workload
registry
parameter
secrets

Environment
ports
volumes
secrets

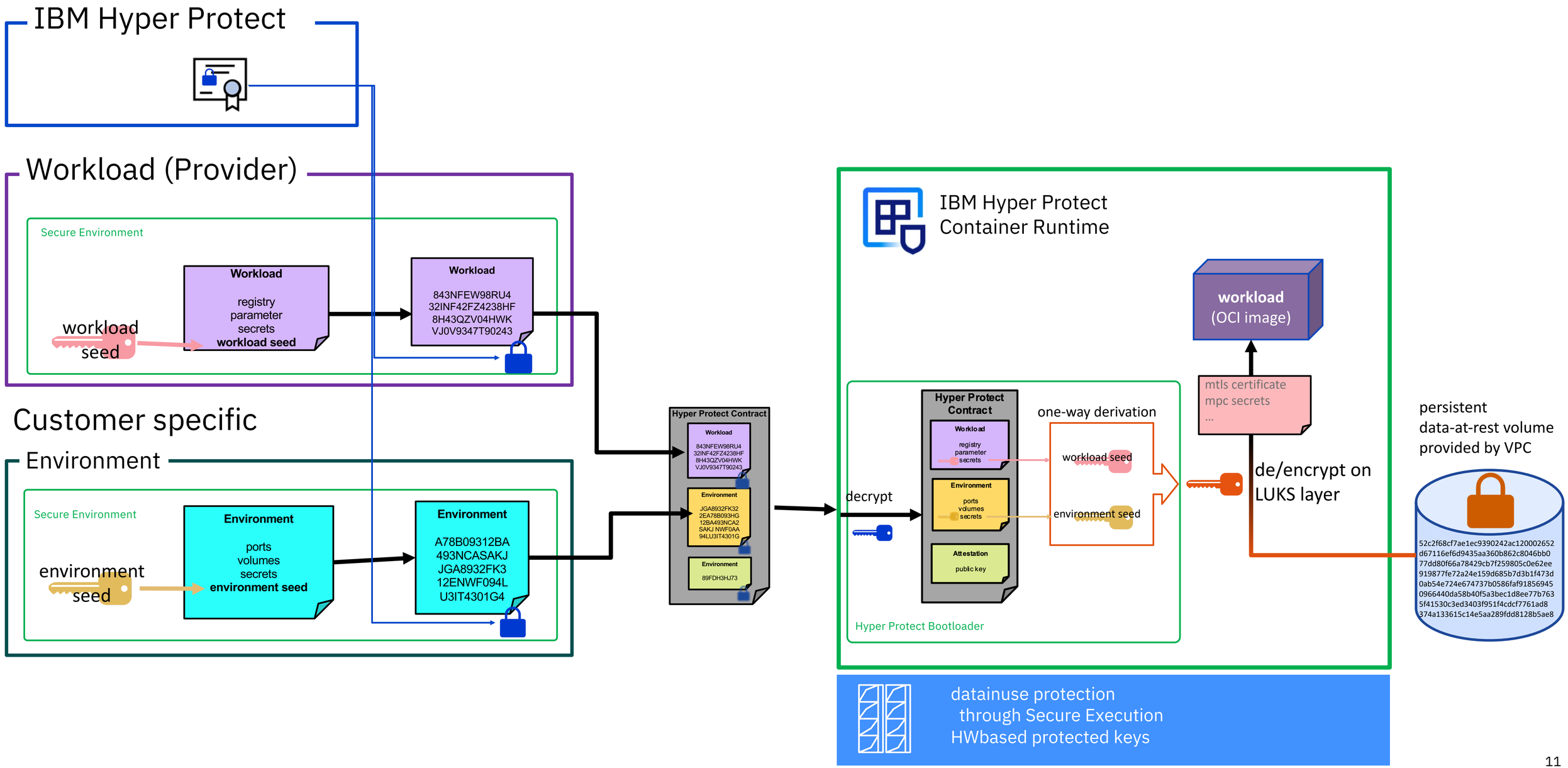
Attestation
public key

attest

encrypt

Built-in Data-at-rest encryption

encryption key derivation within enclave with customer and workload provided seeds



Application workload provisioning

IBM Hyper Protect Container Runtime image provides the Secure KVM guest

This image provides a container runtime and starts your OCI container images

You specify a “contract” at instance provisioning that contains a Docker Compose file or a Pod Descriptor file specifying your application workload

This contract can be in plain text, or encrypted by one or more parties, or encrypted and signed

Auditors can be given the ability to attest that the workload deployed is the expected workload and has not been tampered with

The “contract” allows you to specify…

Docker Compose file or Pod Descriptor file *required*

Logging information *required*

Environmental variables for your workload

Signature over the contract
- You specify your public key so that the container runtime image can verify your signature

Credentials for registry if your OCI images are in a private registry

Public key to verify your OCI image signatures if they are signed

Public key for auditor which allows the attestation record to be encrypted

Seeds for data volume encryption—two seeds are used to create a LUKS key, provided by different personas (workload provider and workload deployer)

IBM Hyper Protect Virtual Servers v2.1
downloadable from Passport Advantage

Hyper Protect Container Runtime
(qcow2-based Kernel Virtual Machine image)

Crypto Express Network API for Secure Execution Enclaves
(Secure Service Container Appliance image)

Standard Virtual Servers

Generic images provided to Hypervisor

Service / Application

Hypervisor (Kernel Virtual Machine with Cloud Init)

Any Management and Middleware*)

Any Linux distro supporting KVM guests and Secure Execution*)

Secure Execution KVM

Service / Application*)

Confidential Computing
OCI-based workload

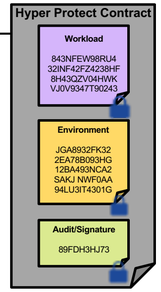
Interfaces no interactive access

Container Runtime
KVM Guest Kernel
Attested deployment
Built to protect data:
in-use, at-rest or in-flight

mTLS

Technical assurance

Encrypted
Multi-party
Contract



Secure Service Container LPAR

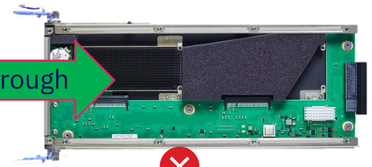
Network API
for Crypto Express Adapter

Crypto Adapter Device Driver

Embedded Linux OS

PCI passthrough

Crypto Express Adapter
HSM in EP 11 mode



Technical assurance (FIPS-certified)

*) Customer-provided. Support restrictions by 3rd party and Linux distribution provider may apply

Additional resources

1

Today’s lab:

https://ibm-wsc.github.io/ConfidentialComputingOnLinuxONE

2

Hyper Protect Virtual Servers 2.1.x product documentation

https://www.ibm.com/docs/en/hpvs/2.1.x

3

IBM view of Confidential Computing

https://www.ibm.com/topics/confidential-computing

4

Secure Execution for Linux documentation

https://www.ibm.com/docs/en/linux-on-systems?topic=virtualization-secure-execution

5

GREP11 documentation

https://cloud.ibm.com/docs/hs-crypto?topic=hs-crypto-grep11-intro

6

Hyper Protect Virtual Servers for Virtual Private Cloud on IBM Cloud

https://cloud.ibm.com/docs/vpc?topic=vpc-about-se

Lab overview

Create a Secure Execution-enabled HPVS 2.1.7 guest running the GREP11 Server. Test end-to-end functionality of GREP11 client code which calls GREP11 Server which in turn calls Crypto Express Network API for Secure Execution Enclaves

1

On your own standard Ubuntu KVM guest, configure rsyslogd service to enable it to receive log messages from your HPVS 2.1.7 GREP11 Server.

2

Perform X509 certificate work to enable mutual TLS authentication between your rsyslogd service and your GREP11 Server.

3

Perform X509 certificate work to enable mutual TLS authentication between your GREP11 Server and the Crypto Express Network API for Secure Execution Enclaves server on the SSC LPAR.

4

Create a signed and encrypted contract in the format HPVS 2.1.7 expects in order to launch your own GREP11 Server as a Secure Execution-enabled HPVS 2.1.7 KVM guest.

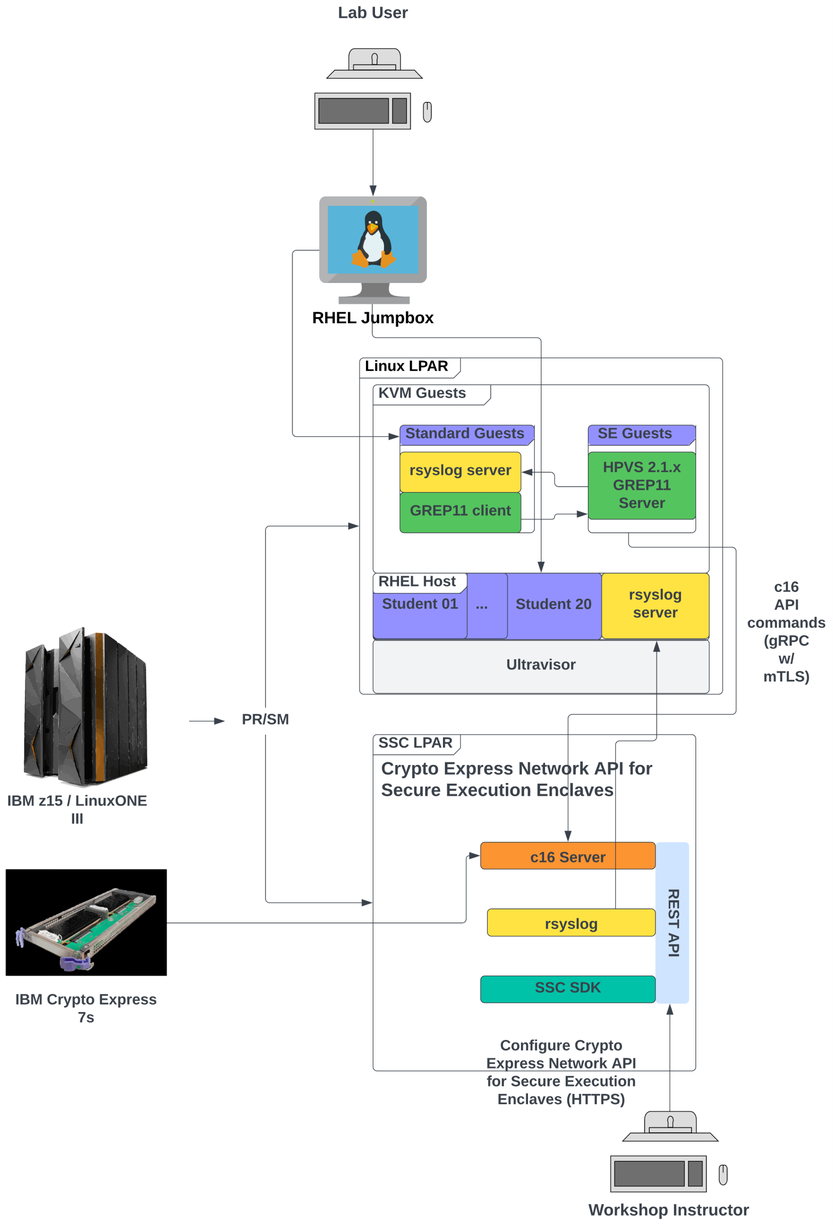
5

Perform X509 certificate work to enable mutual TLS authentication between GREP11 client code and your GREP11 Server.

6

Configure GREP11 client code to request service from your GREP11 Server and perform an end-to-end test of your setup.

Lab topology



The IBM Hyper Protect Platfrom Generation 2

A technical overview

by Stefan Amann, Timo Kußmaul, Carsten Leue, Stefan Liesche, Anbazhagan Mani, Asha Shekarappa, Divya Knoor, Nicolas Mäding, James Magowan, Peter Morjan and Stefan Schmitt

Table of Contents

https://www.ibm.com/downloads/cas/GPVMWPM3

Thank you.