Chains of trust in Confidential Computing
Knowing and verifying what you run

Christophe de Dinechin
Senior Principal Software Engineer
cddd@redhat.com
Agenda

Key topics we are going to cover today

• Overview of Confidential Computing
• What is Attestation?
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
- From root of trust to actual trust
- Platform-specific details
Agenda

Key topics we are going to cover today

• Overview of Confidential Computing
• What is Attestation?
• Use cases for Confidential Computing
• From root of trust to actual trust
• Platform-specific details
• Supporting technologies

• See blog for more details
Chains of trust in Confidential Computing
Knowing and verifying what you run

Christophe de Dinechin
Senior Principal Software Engineer
cddd@redhat.com
Agenda

Key topics we are going to cover today
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
Chains of trust in Confidential Computing
Knowing and verifying what you run

Christophe de Dinechin
Senior Principal Software Engineer
cdd@redhat.com
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
Agenda
Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
Agenda
Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
- From root of trust to actual trust
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
- From root of trust to actual trust
- Platform-specific details
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
- From root of trust to actual trust
- Platform-specific details
- Supporting technologies
Agenda

Key topics we are going to cover today

- Overview of Confidential Computing
- What is Attestation?
- Use cases for Confidential Computing
- From root of trust to actual trust
- Platform-specific details
- Supporting technologies

- See blog for more details
Confidential Computing
Protecting data in-use
I compromised the confidentiality of their proprietary software to advance my agenda of becoming the best at breaking through the lock.

Kevin Mitnick
Problem Statement

Why should infrastructure see your data?

Software now runs on hardware you do not own, like a cloud provider.
Problem Statement

Why should infrastructure see your data?

Hardware resources are owned by the host

Virtual machine host

Physical resources
Problem Statement

Why should infrastructure see your data?

Containers carve out resources from the host

Containers

Virtual machine host

Physical resources
Problem Statement
Why should infrastructure see your data?
Problem Statement

Why should infrastructure see your data?

The host can freely peek inside the container, for example read its memory.
Problem Statement
Why should infrastructure see your data?

For that reason, multiple tenants do not want to share hardware when processing sensitive data.
Problem Statement

Why should infrastructure see your data?

Data on disk or in network is already encrypted today, so the VM host cannot read it nor tamper with it.
Problem Statement
Why should infrastructure see your data?

In non-CC architectures, data in memory is not encrypted, so it can be accessed by the host.
Problem Statement
Why should infrastructure see your data?

Containers
Virtual machine host
Physical resources
Integrity ensures the host cannot corrupt nor poison CPU state or RAM contents

Problem Statement

Why should infrastructure see your data?
Problem Statement

Why should infrastructure see your data?

Attestation proves where you are running and what you are running.
Root of Trust
First there was the hardware

- Workload
  - Linux Kernel
    - Boot Manager
      - BIOS Phase 2
        - BIOS Phase 1
          - ROM-based boot
            - Root of Trust (TPM)
Trust domains

Example: confidential containers

Trusted platform:
Offers confidentiality guarantees enforced by hardware cryptography

Host:
Manages and offers resources used to run containers (CPU, memory, I/O, etc)

Tenant:
Confidential area, inaccessible to the host even when running on it
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
- Does not protect disk, network data, ...

[Image of a hard drive with a cracked cover]
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
- Does not protect disk, network data, ...
- Does not offer any guarantee of service
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
- Does not protect disk, network data, ...
- Does not offer any guarantee of service
- Hardware-based, real-time cryptography
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
- Does not protect disk, network data, ...
- Does not offer any guarantee of service
- Hardware-based, real-time cryptography
- Is highly implementation-dependent
Guarantees

What does confidential computing really provide?

- Confidential computing is about... confidentiality
- Protect data in use from leaks or tampering
- Does not protect against crashes
- Does not protect disk, network data, ...
- Does not offer any guarantee of service
- Hardware-based, real-time cryptography
- Is highly implementation-dependent

TL;DR: There is no automatic security
What is Attestation?

Proving that you run what you want to run where you want to run it
A little bit of terminology

The RATS model (from IETF)

- **Attester**
  - Evidence

- **Endorser**
  - Endorsements

- **Reference Value Provider**
  - Reference values

- **Verifier owner**
  - Appraisal policy (evidence)

- **Relying party owner**
  - Appraisal policy (attestation results)

- **Verifier**
  - Attestation results
Attestation: Basic concepts
Offering proofs about the configuration of a system

- In general, attestation proves a property of a system.
Attestation: Basic concepts

Offering proofs about the configuration of a system

- In general, attestation proves a property of a system
- Remote attestation decouples evidence from verification
Attestation: Basic concepts
Offering proofs about the configuration of a system

• In general, attestation proves a property of a system
• Remote attestation decouples evidence from verification
• Passport check model: present evidence
Attestation: Basic concepts
Offering proofs about the configuration of a system

- In general, attestation proves a property of a system
- Remote attestation decouples evidence from verification
- Passport check model: present evidence
- Background check mode: validate evidence
REMTIS pipeline
A simplified (simplistic?) model of trust chains

Root of trust
Certificates
Endorsement
Signing keys
Measurement
Hashes
Identity
Reference values
Trust
Policies
Secrets
Encryption keys
REMITS pipeline examples
Some simple applications of the REMITS pipeline

Secure Boot: TPM, Manufacturer, Firmware, bootloader, Signed attestation, Attestation policies, Cloud API secret

Selling a property: Notary, Signed records, Deed or affidavit, Property description, I got your money, Handing the keys

Historical money: Gold or silver, Government, Market value, Number of dollars, Handing over cash, Getting food or goods
Attestation

Measuring what we run using cryptography

Preattestation:
Measure the payload before allowing it to start (original SEV)
Attestation
Measuring what we run using cryptography

Prewatention:
Measure the payload before allowing it to start (original SEV)
Postwatention:
Code in the payload can confirm its identity using the measurement in order to get secrets
Attestation
Measuring what we run using cryptography

Preactestation:
Measure the payload before allowing it to start (original SEV)

Postattestation:
Code in the payload can confirm its identity using the measurement in order to get secrets

Workload attestation
The workload itself is attested, e.g. gets secrets from attestation
Use Cases

Various ways to deploy confidential computing
Use Cases
From virtual machine to whole clusters

- Base: Confidential Virtual Machines
Use Cases
From virtual machine to whole clusters

- Base: Confidential Virtual Machines
- Functions: Confidential Workloads (krunvm)

**krunvm**

krunvm is a CLI-based utility for creating microVMs from OCI images, using libkrun and buildah.

**Features**

- Minimal footprint
- Fast boot time
- Zero disk image maintenance
- Zero network configuration
- Support for mapping host volumes into the guest
- Support for exposing guest ports to the host
Use Cases
From virtual machine to whole clusters

- Base: Confidential Virtual Machines
- Functions: Confidential Workloads (krunvm)
- Orchestrated: Confidential Containers
Use Cases

From virtual machine to whole clusters

- Base: Confidential Virtual Machines
- Functions: Confidential Workloads (krunvm)
- Orchestrated: Confidential Containers
- Enchilada: Confidential Clusters
Confidential Virtual Machines
The basic technology behind it all

- New hardware / firmware ABI with new features
- Host kernel no longer trusted, exposes new devices
- Hypervisor no longer trusted, exposes new features
- VM becomes a confidential enclave
- Guest firmware and boot sequence is measured
- Guest kernel can be measured
Confidential Workloads
Lightweight, quick, container-like

- VM as a library (libkrun)
- Direct integration with Podman
- Got very early support for SEV
- First working attestation
Confidential Containers with Kata

Using confidential VMs as a Kubernetes runtime
Confidential Containers with Kata
Using confidential VMs as a Kubernetes runtime
Confidential Clusters
Running an entire cluster inside confidential enclaves

- Make the whole cluster confidential
- Works at the cloud provider level
- Generates confidential nodes
- Attested TLS (ATLS)
- JoinService: Attest nodes
- VerificationService: User-facing
Building actual trust
Keeping the trust alive along the way
How does attestation work?
Challenge / response to deliver secrets

Cryptographic measurement:
Measurement of relevant memory performed by hardware / firmware
How does attestation work?

Challenge / response to deliver secrets

Cryptographic measurement:
Measurement of relevant memory performed by hardware / firmware

Cryptographic challenge:
Send proof of identity (salted)
How does attestation work?

Challenge / response to deliver secrets

Cryptographic measurement:
Measurement of relevant memory performed by hardware / firmware

Cryptographic challenge:
Send proof of identity (salted)

Secret delivery
Ensure the workload cannot do harm if not attested
How does attestation work?

Challenge / response to deliver secrets

Container

Kata Agent

VM (Linux)

Hypervisor (qemu)

Runtime (shim-v2)

Relying party

Key broker

Attestation service

Cryptographic measurement:
Measurement of relevant memory performed by hardware / firmware

Cryptographic challenge:
Send proof of identity (salted)

Secret delivery
Ensure the workload cannot do harm if not attested

Remote attestation:
Can invalidate workloads e.g. if compromised
Attestation flow
Unlock workloads by giving secrets

- Attester sends request

Diagram:
- Attester
- Relying party
- Verifier
- Secrets Broker

Request
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
- Evidence relayed to verifier
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
- Evidence relayed to verifier
- Attestation result returned
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
- Evidence relayed to verifier
- Attestation result returned
- Secrets retrieved
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
- Evidence relayed to verifier
- Attestation result returned
- Secrets retrieved
- Response sent to attester
Attestation flow
Unlock workloads by giving secrets

- Attester sends request
- Response is a cryptographic challenge
- Attester presents crypted evidence
- Evidence relayed to verifier
- Attestation result returned
- Secrets retrieved
- Response sent to attester
Who proves what to whom?
Different kinds of proof for different consumers

- System-facing: System software building a trusted execution environment
- User-facing: User checking if a system is trusted
- Workload-facing: Workload checking if runtime environment is trusted
- Peer-facing: Workloads checking of other workload is trusted
- Cluster-facing: nodes in a cluster check each other
Platform-specific details

Beyond that point, there be zombies
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
Vendor landscape

Different vendors with different approaches?

- **AMD:** Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
- Intel: Trusted Domain Extensions (TDX)
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
- Intel: Trusted Domain Extensions (TDX)
- IBM S390: Secure Execution (SE)
Vendor landscape
Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
- Intel: Trusted Domain Extensions (TDX)
- IBM S390: Secure Execution (SE)
- Power: Protected Execution Facility (PEF)
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)

- Intel: Trusted Domain Extensions (TDX)

- IBM S390: Secure Execution (SE)

- Power: Protected Execution Facility (PEF)

- Arm: Confidential Computing Architecture (CCA)
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
- Intel: Trusted Domain Extensions (TDX)
- IBM S390: Secure Execution (SE)
- Power: Protected Execution Facility (PEF)
- Arm: Confidential Computing Architecture (CCA)
- All these technologies are based on virtualization
Vendor landscape

Different vendors with different approaches?

- AMD: Secure Encrypted Virtualization (SEV)
  - SEV-ES adds Encrypted State (e.g. CPU register file)
  - SEV-SNP adds Secure Nested Pages (integrity protection)
- Intel: Trusted Domain Extensions (TDX)
- IBM S390: Secure Execution (SE)
- Power: Protected Execution Facility (PEF)
- Arm: Confidential Computing Architecture (CCA)
- All these technologies are based on virtualization
- They all work differently
AMD SEV
Secure Encrypted Virtualization

- First generation technology, somewhat flawed
- Provides memory encryption through hardware
- Built on top of virtualization (unlike SME)
- Relies on a separate security processor
- Only features pre-attestation
- Several vulnerabilities gave it a bad reputation
AMD SEV-ES and SEV-SNP

Encrypted State, Secure Nested Pages

- ES protects CPU state from tampering
- No major impact on the (pre-) attestation model
- SNP protects against malicious page mapping
- Can get attestation quote from within the guest
- VMPL gives additional protection levels for VMs
- VMPLs enable protected services, e.g. vTPM
Intel TDX (and SGX)

Trust Domain Extensions (Software Guard Extensions)

- SGX is designed to create "Secure Enclaves"
- TDX is virtualization-based (like AMD-SEV)
- No separate security processor
- New CPU mode, Secure Arbitration Mode (SEAM)
- Various binary modules expose required services
Intel TDX (and SGX)
Trust Domain Extensions (Software Guard Extensions)

- SGX is designed to create "Secure Enclaves"
- TDX is virtualization-based (like AMD-SEV)

- No separate security processor
- New CPU mode, Secure Arbitration Mode (SEAM)
- Various binary modules expose required services
- Attestation performed by a Quoting Enclave
Supporting technologies
The flavor is in the details
How do we get this to work?
Host, Guest, Firmware and Hypervisor support

- Host and guest Linux kernel support
- Hypervisor support
- Guest firmware support
- Host provisioning and support tools, e.g. sevctl
- Generic key brokering and attestation
- Compatibility layers, virtual TPM, SVSM
- Referring you to the blog for pointers
Upcoming attractions

Watch out for these upcoming KVM Forum talks:

- 2:00 Trusted I/O (Jeremy Powell)
- 2:30 Secure VM Service Module (Jörg Rödel)
- 3:00 Zero-trust virtual TPM (Claudio Carvalho)
Conclusion
Attestation means many different things.
Key takeaways

Attestation? We only scratched the surface!

- Confidential Computing is a large collection of technologies
- Attestation can mean very different things even in a same context
- Preserving chains of trust requires careful thinking
- Technologies are not consistent

- Please see blog for more details and links
Thank you

Now is a good time for questions

This Tao3D presentation is available at https://github.com/c3d/presentations (branch kvm-2023-chains-of-trust)