NIST

International Workshop on FAIR Containerized Computational Software

Hardware-Enabled Security for Container Platforms

Mike Bartock

December 5, 2023

AGENDA

- Hardware Platform Security Overview
- NIST Publications
  - NIST IR 8320 Hardware-enabled Security: Enabling A Layered Approach To Platform Security
  - NIST IR 8320A Hardware-Enabled Security: Container Platform Security Prototype
  - NIST IR 8320B Hardware-Enabled Security: Policy-Based Governance in Trusted Container Platforms
  - NIST IR 8320C Hardware-Enabled Security: Machine Identity Management and Protection
  - Q&A

HARDWARE PLATFORM SECURITY OVERVIEW

- Increased software security leads attackers to pushing lower in the platform stack:
  - Modification of platform firmware
  - Supply chain interception through physical replacement of firmware or hardware
  - Access to data or execution of code outside of regulated geopolitical or other boundaries
  - Circumvention of software and/or firmware-based security mechanisms

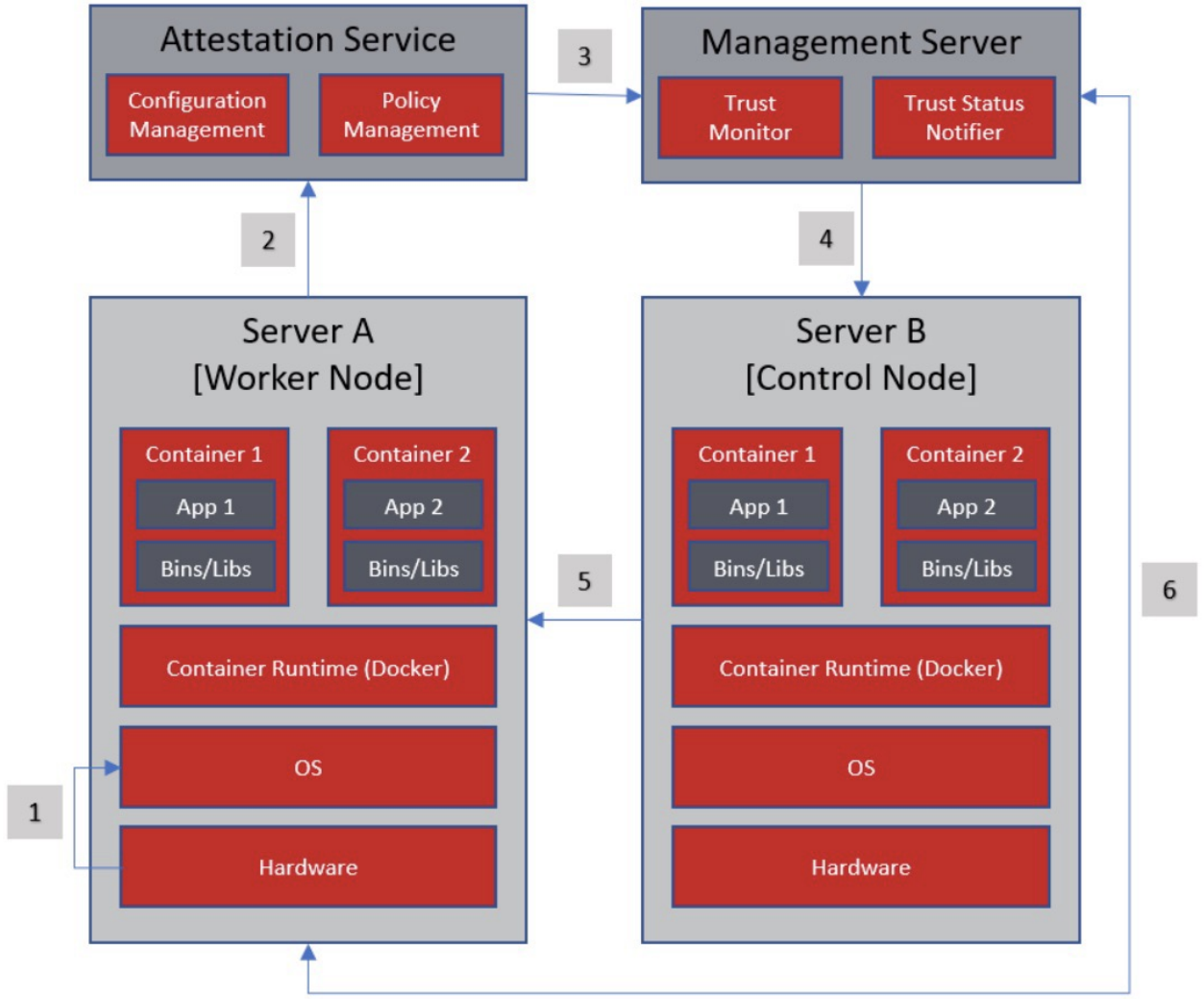
NIST IR 8320 PRINCIPLES

- Platform Integrity Verification
  - Cryptographic measurement of software and firmware
  - Firmware and configuration verification
  - Hardware Security Module (HSM)
  - The Chain of Trust (CoT) - method for maintaining valid trust boundaries by applying a principle of transitive trust
  - Supply Chain Protection
- Data Protection and Confidential Computing
  - Protecting and securing data while in use
  - Trusted Execution Environment (TEE) is an area or enclave protected by a system processor
  - Memory Isolation - encrypt content running in platform memory
  - Application Isolation - protect the memory reserved for an individual application

NIST IR 8320 PRINCIPLES (CONT'D)

- Remote Attestation Services
  - Collate server information and measurement details
  - Platform Attestation - collected host data is compared and verified against policies
  - Remote TEE Attestation
  - Can be integrated with workload orchestrator

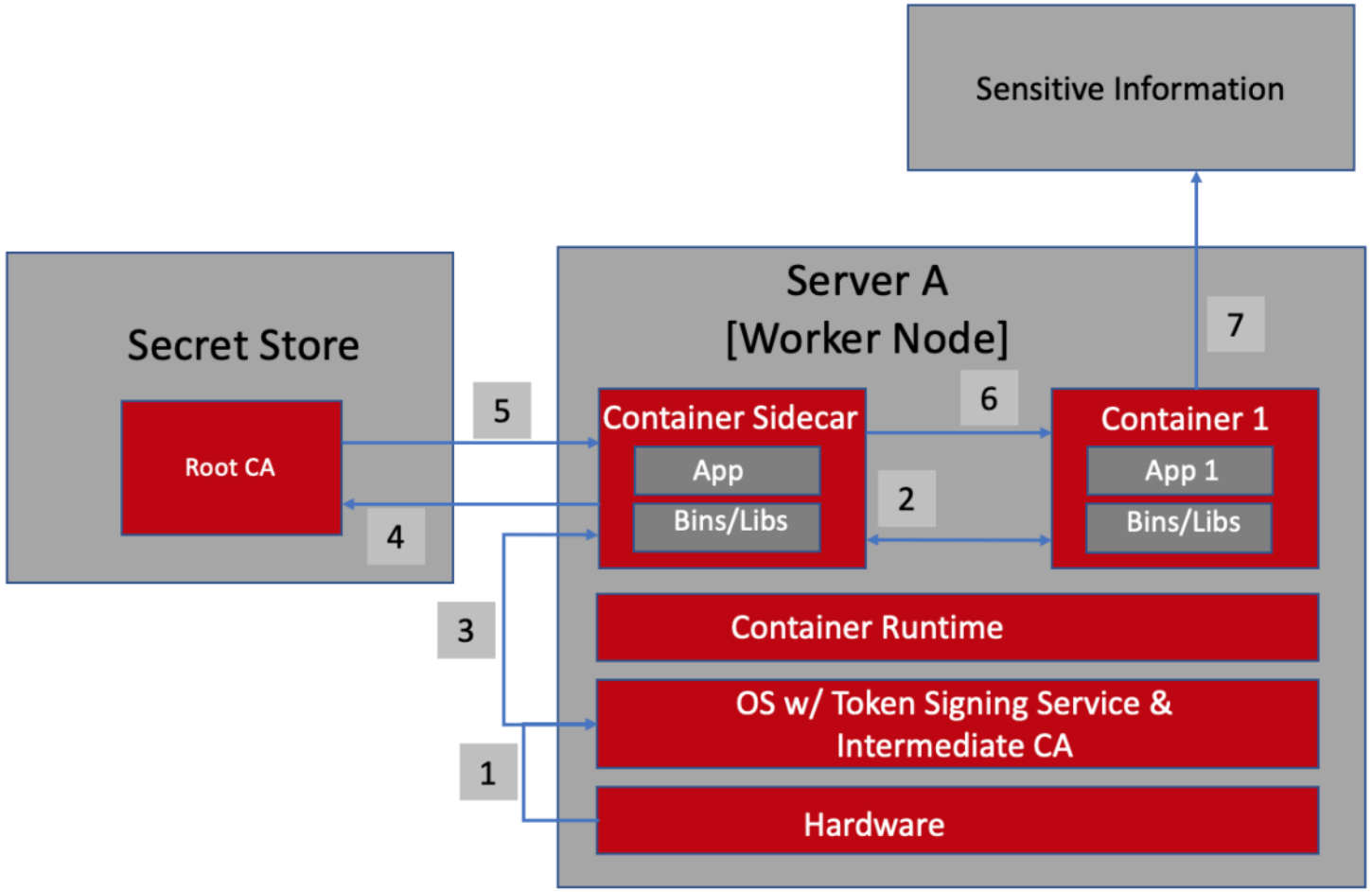
NIST IR 8320A: PROTOTYPE WORKLOAD PLACEMENT ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Integration with Orchestrator

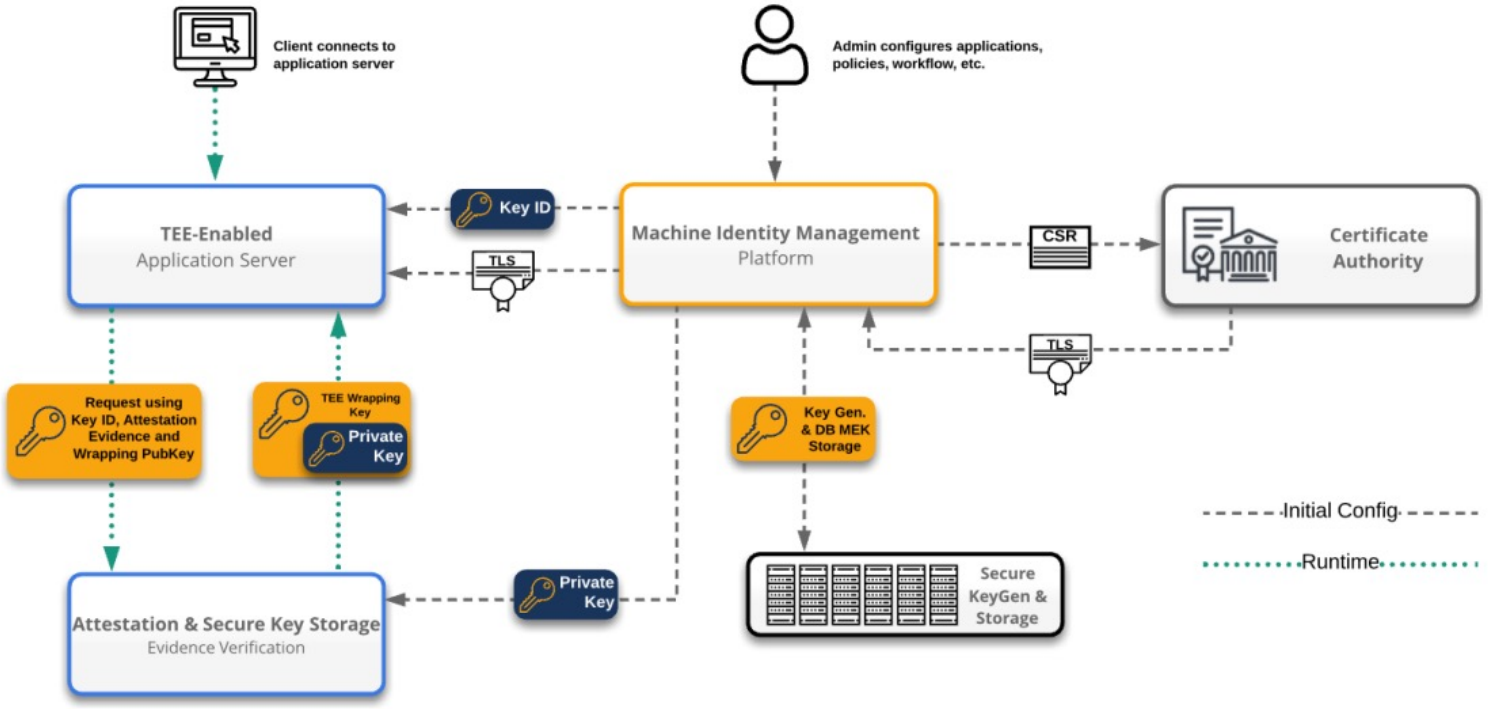
NIST IR 8320B: PROTOTYPE APPLICATION IDENTITY ARCHITECTURE



Principles Included:

- TPM
- Chain of Trust
- Asset Tagging
- Remote Attestation Services
- Workload Encryption
- Integration with Orchestrator

NIST IR 8320C: PROTOTYPE CONFIDENTIAL COMPUTING ARCHITECTURE



Principles Included:

- TEE
- Memory Isolation
- Remote TEE Attestation
- Integration with Orchestrator

REFERENCES

- https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud
- NIST IR 8320: Hardware-Enabled Security:Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases
  - https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320-draft.pdf
- NIST IR 8320A Hardware-Enabled Security: Container Platform Security Prototype
  - https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320A.pdf
- NIST IR 8320B Hardware-Enabled Security: Policy-based Governance In Trusted Container Platforms
  - https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320B.pdf
- Draft NIST IR 8320C Hardware-Enabled Security: Machine Identity Management And Protection
  - https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8320C.ipd.pdf
- Draft NIST IR 8320D Hardware-Enabled Security: Hardware-Based Confidential Computing
  - https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8320D.ipd.pdf

- Contact hwsec@nist.gov

Questions?