

CLAIMS

1. A computing system comprising:
one or more processors; and
one or more computer-readable storage medium having stored computer executable instructions which are executable by the one or more processors for implementing a method for creating a container-based memory enclave, the method comprising:

identifying a container image having a security component that is used for attesting to a particular security configuration that is used by a host system running on a first security domain, the security component being stored at a memory address of the host system;

using the container image to instantiate a new container, the new container being configured to utilize enclave memory in a second security domain of a host system based on a security component stored at an address of the host system, the new container including a copy of the security component with a particular memory address that is a purported link from the container to the memory address of the security component stored at the host system; and

during or after instantiation of the new container, modifying the purported link from the container to the particular memory address of the security component stored at the host system so that the purported link from the container to the memory address is modified to verifiably link the container to the memory address of the host system.

2. The computing system of claim 1, wherein the modifying the purported link comprises overwriting the particular address of the security component at the new container with the address of the host system where the security component used by the host system is loaded.

3. The computing system of claim 1, wherein the modifying the purported link comprises creating a link from the particular address of the security component at the new container to the address of the host system where the security component used by the host system is loaded.

4. The computing system of claim 1, wherein the modifying the purported link comprises updating a referenced address in a mapping table associated with the particular address to include or reference the address of the host system where the security component used by the host system is loaded.

5. The computing system of claim 4, wherein the method further includes creating the mapping table and, during or after instantiating the new container, using metadata associated with the new container to add the referenced address to the mapping table.

6. The computing system of claim 1, wherein the security component comprises a library file.

7. The computing system of claim 1, wherein the security component includes data that is used to generate an attestation report regarding the security configuration for the new container.

8. The computing system of claim 7, wherein the method further includes performing attestation of security guarantees associated with the security configuration for the new container.

9. A computing system comprising:
one or more processors; and
one or more computer-readable storage medium having stored computer executable instructions which are executable by the one or more processors for implementing a method for performing attestation for a container-based memory enclave, the method comprising:

identifying one or more containers, each of the one or more containers being configured to reference enclave memory residing in a security domain that is different than a first security domain of the host system and using a security component for attesting to a particular security configuration for the enclave memory, the security component being loaded at a memory address of the host system and being linked to by one or more references to the security component at the one or more containers;

obtaining a single attestation report from a remote attestation service regarding security guarantees of a security configuration of the one or more containers based on the security component;

receiving a request to attest to the security guarantees for a particular container of the one or more containers subsequent to receiving the single attestation report from the remote attestation service; and

attesting to the security guarantees for the particular container based on the single attestation report that was received prior to the receiving of the request to attest.

10. The computing system of claim 9, wherein the method further includes attesting to the security guarantees for a plurality of containers that each include a reference to the security component loaded at the memory address of the host system based on the single attestation report.

11. The computing system of claim 10, wherein the single attestation report is obtained in response to a request to attest to a security guarantee of a different container having a reference to the security component loaded at the address of the host.

12. The computing system of claim 9, wherein the method further includes:
receiving a new attestation request for a particular container having allocated enclave memory, which is generated subsequent to a reallocation of the allocated enclave memory for the container; and

validating integrity of the container and issuing a new attestation report without requiring the new attestation request to be submitted to a remote attestation service.

13. The computing system of claim 9, wherein the method further includes:
monitoring container state and disabling a container that is determined to be compromised.

14. The computing system of claim 9, wherein the method further includes:
upon receiving a subsequent container attestation request, determining an attribute of a particular container associated with the subsequent container attestation request; and

deterministically routing the subsequent container attestation request to a remote service based on the attribute of the particular container or, alternatively generating an attestation report without routing the subsequent container attestation request to the remote service based at least in part on the attribute of the particular container.

15. The computing system of claim 14, wherein the attribute of the subsequent container comprises a longevity of the container and a first set of containers have a relatively greater longevity than a second set of containers, wherein one or more container attestation requests associated with the first set of containers are routed to the remote service, while one or more attestation report is generated for each of the second set of containers, including the subsequent container, which have a relatively shorter longevity than the first set of containers, without routing the second set of containers to the remote service.