CLAIMS

1. A method comprising:

receiving, at a secure interface control of a computer system, an access request for a data structure related to a secure entity in a secure domain of the computer system, wherein the secure interface control comprises firmware, hardware, trusted software or a combination of firmware, hardware, and trusted software;

checking, by the secure interface control, for a virtual storage address associated with a location of the data structure, wherein checking for the virtual storage address further comprises inspecting a zone-security table to determine whether a virtual address compare indicator associated with a host virtual address is enabled or disabled, wherein the zone-security table comprises one entry for each page of host absolute storage, each entry is indexed by a host absolute address, and each entry comprises information to verify the entry as belonging to the secure entity;

verifying, by the secure interface control, a mapping of the virtual storage address provided by the non-secure entity based on determining that the virtual address compare indicator is enabled;

requesting, by the secure interface control, an address translation using a virtual address space of a non-secure entity of the computer system based on determining that the location of the data structure is associated with the virtual storage address; and

accessing, by the secure interface control, the data structure based on a result of the address translation.

2. The method of claim 1, further comprising: accessing, by the secure interface control, the data structure using an absolute address based on a determining that the location of the data structure is not associated with the virtual storage address.

3. The method of claim 1, wherein verifying the mapping of the virtual storage address comprises checking for a change in the mapping compared to a previous mapping.

4. The method of claim 1, wherein the data structure related to the secure entity in the secure domain is distributed between a plurality of pages of memory.

5. The method of claim 4, wherein one or more pages of memory donated by the non-secure entity reside at a contiguous range of virtual addresses.

6. The method of claim 1, wherein the non-secure entity comprises a hypervisor configured to host one or more secure guests as the secure entity.

7. A system comprising:

a memory;

a processing unit; and

a secure interface control comprising firmware, hardware, trusted software or a combination of firmware, hardware, and trusted software, the secure interface control configured to perform a plurality of operations comprising:

receiving an access request for a data structure related to a secure entity in a secure domain;

checking for a virtual storage address associated with a location of the data structure in the memory, wherein checking for the virtual storage address further comprises inspecting a zone-security table to determine whether a virtual address compare indicator associated with a host virtual address is enabled or disabled, wherein the zone-security table comprises one entry for each page of host absolute storage, each entry is indexed by a host absolute address, and each entry comprises information to verify the entry as belonging to the secure entity;

verifying a mapping of the virtual storage address provided by the non-secure entity based on determining that the virtual address compare indicator is enabled; requesting an address translation using a virtual address space of a non-secure entity of the processing unit based on determining that the location of the data structure is associated with the virtual storage address; and

accessing the data structure based on a result of the address translation.

8. The system of claim 7, wherein the secure interface control is configured to perform operations comprising: accessing the data structure using an absolute address based on a determining that the location of the data structure is not associated with the virtual storage address.

9. The system of claim 7, wherein verifying the mapping of the virtual storage address comprises checking for a change in the mapping compared to a previous mapping.

10. The system of claim 7, wherein the data structure related to the secure entity in the secure domain is distributed between a plurality of pages of the memory.

11. The system of claim 10, wherein one or more pages of memory donated by the non-secure entity reside at a contiguous range of virtual addresses.

12. The system of claim 7, wherein the non-secure entity comprises a hypervisor configured to host one or more secure guests as the secure entity.

13. A computer program product comprising a computer readable storage medium, the computer readable storage medium comprising computer executable instructions, which when executed by a secure interface control of a processing unit causes the processing unit to perform a method comprising:

receiving, at the secure interface control, an access request for a data structure related to a secure entity in a secure domain, wherein the secure interface control comprises firmware, hardware, trusted software or a combination of firmware, hardware, and trusted software;

checking, by the secure interface control, for a virtual storage address associated with a location of the data structure, wherein checking for the virtual storage address further comprises inspecting a zone-security table to determine whether a virtual address compare indicator associated with a host virtual address is enabled or disabled, wherein the zone-security table comprises one entry for each page of host absolute storage, each entry is indexed by a host absolute address, and each entry comprises information to verify the entry as belonging to the secure entity;

verifying, by the secure interface control, a mapping of the virtual storage address provided by the non-secure entity based on determining that the virtual address compare indicator is enabled;

requesting, by the secure interface control, an address translation using a virtual address space of a non-secure entity based on determining that the location of the data structure is associated with the virtual storage address; and

accessing, by the secure interface control, the data structure based on a result of the address translation.

14. The computer program product of claim 13, wherein the executable instructions further cause the processing unit to perform: accessing, by the secure interface control, the data structure using an absolute address based on a determining that the location of the data structure is not associated with the virtual storage address.

15. The computer program product of claim 13, wherein verifying the mapping of the virtual address comprises checking for a change in the mapping compared to a previous mapping.

16. The computer program product of claim 13, wherein the data structure related to the secure entity in the secure domain is distributed between a plurality of pages of memory.

17. The computer program product of claim 16, wherein one or more pages of memory donated by the non-secure entity reside at a contiguous range of virtual addresses.

18. The computer program product of claim 13, wherein the non-secure entity comprises a hypervisor configured to host one or more secure guests as the secure entity.