CLAIMS

1. A method comprising:

receiving a secure access request for a secure page of memory at a secure interface control of a computer system;

checking, by the secure interface control, a disable virtual address compare state associated with the secure page~~; and~~, wherein the disable virtual address compare state is stored and updated through a zone-security table maintained by the secure interface control, the zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state;

disabling, by the secure interface control, a virtual address check in accessing the secure page to support mapping of a plurality of virtual addresses to a same absolute address to the secure page based on the disable virtual address compare state being set;

verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier;

confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and

terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.

~~2. The method of claim 1, further comprising:~~

~~verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier.~~

~~3.~~2. The method of claim ~~2~~1, wherein the domain identifier of the secure domain is compared to a plurality of domain identifiers of the secure domains identified as allowing sharing to confirm authorization to access the shared page.

~~4. The method of claim 2, further comprising:~~

~~confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page,~~

~~wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and~~

~~terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.~~

~~5. The method of claim 1, wherein the disable virtual address compare state is stored and updated through a zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state.~~

~~6.~~3. The method of claim 1, wherein the secure interface control comprises firmware, hardware, trusted software or a combination of firmware, hardware, and trusted software and the secure page is assigned to a secure virtual machine or a secure container managed by a hypervisor or operating system.

4. The method of claim 1, wherein the zone security table is indexed by absolute address.

~~7.~~5. A system comprising:

a memory;

a processing unit; and

a secure interface control configured to perform a plurality of operations comprising:

checking a disable virtual address compare state associated with a secure access request for a secure page of the memory from an entity executing on the processing unit~~; and~~, wherein the disable virtual address compare state is stored and updated through a zone-security table maintained by the secure interface control, the zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state;

disabling a virtual address check in accessing the secure page to support mapping of a plurality of virtual addresses to a same absolute address to the secure page based on the disable virtual address compare state being set~~.~~;

verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier;

confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and

terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.

~~8. The system of claim 7, wherein the secure interface control is configured to perform operations comprising:~~

~~verifying that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier.~~

~~9.~~6. The system of claim ~~8~~5, wherein the domain identifier of the secure domain is compared to a plurality of domain identifiers of the secure domains identified as allowing sharing to confirm authorization to access the shared page.

~~10. The system of claim 8, wherein the secure interface control is configured to perform operations comprising:~~

~~confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and~~

~~terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.~~

~~11. The system of claim 7, wherein the disable virtual address compare state is stored and updated through a zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state.~~

~~12~~7. The system of claim ~~7~~5, wherein the secure interface control comprises firmware, hardware, trusted software or a combination of firmware, hardware, and trusted software and the secure page is assigned to a secure virtual machine or a secure container managed by a hypervisor or operating system.

8. The system of claim 5, wherein the zone security table is indexed by absolute address.

~~13~~9. 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:

checking a disable virtual address compare state associated with a secure access request for a secure page of memory from an entity executing on the processing unit~~; and~~, wherein the disable virtual address compare state is stored and updated through a zone-security table maintained by the secure interface control, the zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state;

disabling a virtual address check in accessing the secure page to support mapping of a plurality of virtual addresses to a same absolute address to the secure page based on the disable virtual address compare state being set~~.~~;

verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier;

confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and

terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.

~~14. The computer program product of claim 13, wherein the executable instructions further cause the processing unit to perform:~~

~~verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier.~~

~~15.~~10. The computer program product of claim ~~14~~9, wherein the domain identifier of the secure domain is compared to a plurality of domain identifiers of the secure domains identified as allowing sharing to confirm authorization to access the shared page.

~~16. The computer program product of claim 14, wherein the executable instructions further cause the processing unit to perform:~~

~~confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and~~

~~terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.~~

~~17. The computer program product of claim 13, wherein the disable virtual address compare state is stored and updated through a zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state.~~

~~18.~~11. The computer program product of claim ~~13~~6, wherein the secure page is assigned to a secure virtual machine or a secure container managed by a hypervisor or operating system.

12. The computer program product of claim 9, wherein the zone security table is indexed by absolute address.

~~19.~~13. A method comprising:

receiving a secure access request for a secure page of memory at a secure interface control of a computer system;

checking, by the secure interface control, a disable virtual address compare state associated with the secure page~~; and~~, wherein the disable virtual address compare state is stored and updated through a zone-security table maintained by the secure interface control, the zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state;

enabling absolute address access to the secure page with no virtual address specified based on an authorization status of an entity making the secure access request and the disable virtual address compare state being set~~.~~;

verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier;

confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and

terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.

~~20. The method of claim 19, further comprising:~~

~~verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier.~~

~~21.~~14. The method of claim ~~20~~13, wherein the domain identifier of the secure domain is compared to a plurality of domain identifiers of the secure domains identified as allowing sharing to confirm authorization to access the shared page.

~~22.~~15. The method of claim ~~19~~13, wherein the secure interface control comprises firmware, hardware, or a combination of firmware and hardware, and the secure page is assigned to a secure container or a secure virtual machine managed by a hypervisor or operating system.

~~23.~~16. A system comprising:

a memory;

a processing unit; and

a secure interface control configured to perform a plurality of operations comprising:

checking a disable virtual address compare state associated with a secure access request for a secure page of the memory from an entity executing on the processing unit~~; and~~, wherein the disable virtual address compare state is stored and updated through a zone-security table maintained by the secure interface control, the zone-security table comprising a secure domain identifier associated with the secure page, virtual address mapping data associated with the secure page, and the disable virtual address compare state;

enabling absolute address access to the secure page with no virtual address specified based on an authorization status of an entity making the secure access request and the disable virtual address compare state being set~~.~~;

verifying, by the secure interface control, that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier;

confirming that a plurality of groups of dynamic-address-translation tables that map virtual addresses to absolute addresses is unchanged by an unsecure host configured to manage one or more of the groups of dynamic-address-translation tables for any of multiple secure domains that have access to the secure page, wherein each table mapping for a virtual address comprises multiple associated tables in the one or more groups of dynamic-address-translation tables; and

terminating the secure access request based on detecting a change in the one or more groups of the dynamic-address-translation tables.

~~24. The system of claim 23, wherein the secure interface control is configured to perform operations comprising:~~

~~verifying that a secure domain of a plurality of secure domains is authorized to access a shared page based on a domain identifier.~~

~~25.~~17. The system of claim ~~24~~16, wherein the domain identifier of the secure domain is compared to a plurality of domain identifiers of the secure domains identified as allowing sharing to confirm authorization to access the shared page.