CLAIMS

1. A method comprising:

receiving (1002), by a secure interface control of a computing system, a request by a requestor to access a page in a memory of the computing system;

responsive to determining (940) if the requestor is a non-secure guest requestor or if the requestor is a secure guest requestor;

responsive to determining (1004) that the requestor is the non-secure guest requestor:

determining (945) if a secure-storage bit is set; and

responsive to the secure-storage bit is set, prohibiting access to the page without performing an authorization check; and

responsive to determining (1006) that the requestor is the secure guest requestor, performing the authorization check.

2. The method of claim 1, wherein the authorization check comprises a check, based on a zone security table (100), to verify that the page belongs to a secure domain that is trying to access the page, wherein the zone security table comprises a secure guest domain identifier (120), a secure interface control bit (130), a disable address compare bit (140), a shared bit (150), and a host virtual address (160).

3. 2. The method of claim 1, wherein the authorization check comprises a check to verify that a mapping by a non-secure entity of the page while the page is resident in memory.

43. The method of claim 1, further comprising:

responsive to a request from an untrusted entity, marking the page as a secure page.

54. The method of claim 43, further comprising:

responsive to marking the page as the secure page, preventing access to the secure page by any untrusted entity.

65. The method of claim 43, further comprising:

prior to marking the page as the secure page and responsive to the request from the untrusted entity, issuing, by the untrusted entity, an import command in preparation for paging-in of the page.

76. The method of claim 1, further comprising:

responsive to a request from an untrusted entity, registering the page as belonging to an associated secure entity and registering an associated host-virtual address.

87. The method of claim 76, further comprising:

responsive to registering the page with the associated secure entity and the associated host-virtual address, preventing access to the secure page by another secure entity or if the host virtual address has changed.

9. The method of claim 6, wherein the secure interface control comprises firmware, hardware, or a combination of firmware and hardware; the untrusted entity comprises a hypervisor; and the secure requestor comprises a virtual machine that is a secure guest hosted by the hypervisor in a secure domain.

10. The method of claim 1, further comprising:

responsive to the authorization check determining that the secure requestor is authorized, granting the secure requestor access to the page.

118. A system comprising:

a memory comprising computer readable instructions; and

a processing device for executing the computer readable instructions for performing a method comprising:

receiving (1002), by a secure interface control of a computing system, a request by a requestor to access a page in a memory of the computing system;

determining (940) if the requestor is a non-secure guest requestor or if the requestor is a secure guest requestor;

responsive to determining (1004) that the requestor is athe non-secure guest requestor:

determining (945) if a secure-storage bit is set; and

responsive to a secure-storage bit being set, prohibiting access to the page without performing an authorization check; and

responsive to determining (1006) that the requestor is athe secure guest requestor, performing the authorization check.

12. The system of claim 11, wherein the authorization check comprises a check, based on a zone security table (100), to verify that the page belongs to a secure domain that is trying to access the page., wherein the zone security table comprises a secure guest domain identifier (120), a secure interface control bit (130), a disable address compare bit (140), a shared bit (150), and a host virtual address (160).

~~13.~~ 9. The system of claim ~~11~~8, wherein the authorization check comprises a check to verify that a mapping by a non-secure entity of the page while the page is resident in memory.

~~14~~10. The system of claim ~~11~~8, wherein the method further comprises:

~~responsive to a request from an untrusted entity, marking the page as a secure page.~~

~~15~~11. The system of claim ~~14~~10, wherein the method further comprises:

~~responsive to marking the page as the secure page, preventing access to the secure page by any untrusted entity.~~

~~16~~12. The system of claim ~~15~~11, wherein the method further comprises:

~~prior to marking the page as the secure page and responsive to the request from the untrusted entity, issuing, by the untrusted entity, an import command in preparation for paging-in of the page.~~

1~~7~~3. A computer program product comprising:

~~a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a processing device to cause the processing device to perform a method~~ as claimed in any of claims 1 to 7.~~comprising:~~

~~receiving, by a secure interface control of a computing system, a request by a requestor to access a page in a memory of the computing system;~~

~~responsive to determining that the requestor is a non-secure requestor and responsive to a secure-storage bit being set, prohibiting access to the page without performing an authorization check; and~~

~~responsive to determining that the requestor is a secure requestor, performing the authorization check.~~

~~18. The computer program product of claim 17, wherein the authorization check comprises a check to verify that the page belongs to a secure domain that is trying to access the page.~~

~~19. The computer program product of claim 17, wherein the authorization check comprises a check to verify that a mapping by a non-secure entity of the page while the page is resident in memory.~~

~~20. The computer program product of claim 17, wherein the method further comprises:~~

~~responsive to a request from an untrusted entity, marking the page as a secure page;~~

responsive to marking the page as the secure page, preventing access to the secure page by any untrusted entity; and

prior to marking the page as the secure page and responsive to the request from the untrusted entity, issuing, by the untrusted entity, an import command in preparation for paging in of the page.

21. The computer program product of claim 15, wherein the method further comprises:

responsive to the authorization check determining that the secure requestor is authorized, granting the secure requestor access to the page.

22. A computer-implemented method comprising:

receiving, by a secure interface control of a computing system, a request by a requestor to access a page in a memory of the computing system;

responsive to determining that the requestor is a non-secure requestor and responsive to a secure-storage bit being set, prohibiting access to the page without performing an authorization check; and

responsive to determining that the requestor is a secure requestor, performing the authorization check,

wherein the authorization check comprises a check to verify that the page belongs to a secure domain that is trying to access the page, and a check to verify that a non-secure entity has not changed a host mapping of the page while the page is resident in the memory.

23. The computer-implemented method of claim 22, wherein the secure interface control comprises firmware, hardware, or a combination of firmware and hardware; and the secure requestor comprises a virtual machine that is a secure guest hosted by a hypervisor in a secure domain.

24. A computer program product comprising:

a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a processing device to cause the processing device to perform a method comprising:

receiving, by a secure interface control of a computing system, a request by a requestor to access a page in a memory of the computing system;

responsive to determining that the requestor is a non-secure requestor and responsive to a secure-storage bit being set, prohibiting access to the page without performing an authorization check; and

responsive to determining that the requestor is a secure requestor, performing the authorization check,

wherein the authorization check comprises a check to verify that the page belongs to a secure domain that is trying to access the page, and a check to verify that a non-secure entity has not changed a host mapping of the page while the page is resident in the memory.

~~25. The computer program product of claim 24, wherein the secure interface control comprises firmware, hardware, or a combination of firmware and hardware; and the secure requestor comprises a virtual machine that is a secure guest hosted by a hypervisor in the secure domain.~~