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;

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, 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).

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.

3. The method of claim 1, further comprising:

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

4. The method of claim 3, further comprising:

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

5. The method of claim 3, 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.

6. 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.

7. The method of claim 6, 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.

8. 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 the 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 the secure guest requestor, performing the authorization check, 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).

9. The system of claim 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.

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

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

11. The system of claim 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.

12. The system of claim 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.

13. 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.