CLAIMS

1. A method comprising:

determining, by a secure interface control of a computer that prevents unauthorized accesses to locations in a memory of the computer, that a host absolute page is not previously mapped to a virtual page in accordance with securing the host absolute page; and

determining, by the secure interface control, that a host virtual page is not already mapped to an absolute page in accordance with securing the host absolute page, wherein the secure interface control:

marks the host absolute page as secure;

registers the host absolute page for use by the secure interface control;

securely decrypts the host absolute page;

registers a host virtual address associated with the host absolute page to create a host-address pair for use by a secure entity;

checks the host-address pair on access by the secure entity; and

locks the host absolute page for use by the secure interface control to prevent other calls to the host absolute page.

2. The method of claim 1, wherein the secure interface control un-registers the host absolute page for use by the secure interface control, and registers the host absolute page to a secure domain.

3. The method of claim 1, wherein the secure interface control unlocks the host absolute page to assign a secure guest domain loaded into the memory.

4. The method of claim 1, wherein the secure entity accesses a secure page that has been transparently paged-in by an untrusted entity executing on the computer and is non-secure.

5. The method of claim 4, wherein the untrusted entity is a hypervisor, and wherein the secure entity is a secure guest.

6. The method of claim 4, wherein hardware presents a program interruption to the untrusted entity indicating a need for decryption of a secure guest page.

7. The method of claim 6, wherein the untrusted entity issues an import instruction that provides the host absolute page and the host virtual page.

8. A computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable to cause operations comprising:

determining, by a secure interface control of a computer that prevents unauthorized accesses to locations in a memory of the computer, that a host absolute page is not previously mapped to a virtual page in accordance with securing the host absolute page; and

determining, by the secure interface control, that a host virtual page is not already mapped to an absolute page in accordance with securing the host absolute page, wherein the secure interface control:

marks the host absolute page as secure;

registers the host absolute page for use by the secure interface control;

securely decrypts the host absolute page;

registers a host virtual address associated with the host absolute page to create a host-address pair for use by a secure entity;

checks the host-address pair on access by the secure entity; and

locks the host absolute page for use by the secure interface control to prevent other calls to the host absolute page.

9. The computer program product of claim 8, wherein the secure interface control un-registers the host absolute page for use by the secure interface control, and registers the host absolute page to a secure domain.

10. The computer program product of claim 8, wherein the secure interface control unlocks the host absolute page to assign a secure guest domain loaded into the memory.

11. The computer program product of claim 8, wherein the secure entity accesses a secure page that has been transparently paged-in by an untrusted entity executing on the computer and is non-secure.

12. The computer program product of claim 11, wherein the untrusted entity is a hypervisor, and wherein the secure entity is a secure guest.

13. The computer program product of claim 11, wherein hardware presents a program interruption to the untrusted entity indicating a need for decryption of a secure guest page.

14. The computer program product of claim 13, wherein the untrusted entity issues an import instruction that provides the host absolute page and the host virtual page.

15. A system comprising:

a memory;

a secure interface control of the system that prevents unauthorized accesses to locations in the memory,

wherein the system performs operations comprising:

determining, by a secure interface control of a computer that prevents unauthorized accesses to locations in a memory of the computer, that

a host absolute page is not previously mapped to a virtual page in accordance with securing the host absolute page; and

determining, by the secure interface control, that a host virtual page is not already mapped to an absolute page in accordance with securing the host absolute page, wherein the secure interface control:

marks the host absolute page as secure;

registers the host absolute page for use by the secure interface control;

securely decrypts the host absolute page;

registers a host virtual address associated with the host absolute page to create a host-address pair for use by a secure entity;

checks the host-address pair on access by the secure entity; and

locks the host absolute page for use by the secure interface control to prevent other calls to the host absolute page.

16. The system of claim 15, wherein the secure interface control un-registers the host absolute page for use by the secure interface control, and registers the host absolute page to a secure domain.