CLAIMS

1. A method comprising:

receiving, by a secure interface control of a system, an initialization instruction from an untrusted entity of the system to set donated storage from the untrusted entity as secure, wherein the untrusted entity facilitates deploying one or more virtual machines on the system, and the secure interface control facilitates the untrusted entity in providing one or more services to the one or more virtual machines;

implementing, by the secure interface control, the initialization instruction through assigning a portion of the donated storage as zone-specific storage and tagging the zone-specific storage with a unique-secure domain for secure control that prevents access by the untrusted entity and the one or more virtual machines; and

assigning, by the secure interface control, secure guest-domain-specific storage and tagging the secure-guest-domain-specific storage as belonging to the secure interface control and qualified with an associated secure-guest-domain, wherein the secure-guest-domain provides secure access to one of the one or more virtual machines and prevents access from the untrusted entity.

2. The method of claim 1, wherein the implementing of the initialization instruction causes the secure interface control to verify the donated storage as non-secure and set the donated storage as secure storage.

3. The method of claim 1, wherein the implementing of the initialization instruction causes the secure interface control to assign a portion of the donated storage to be defined as absolute storage and tag this portion of the donated storage as having no associated virtual address.

4. The method of claim 1, wherein the implementing of the initialization instruction causes the secure interface control to assign a portion of the donated storage to be defined as virtual storage and tag this portion of the donated storage with an associated virtual address.

5. The method of claim 1, wherein the donated storage is registered to the secure interface control and the donated storage is marked as secure.

6. The method of claim 1, the method further comprising:

implementing, by the secure interface control, a create configuration instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

7. The method of claim 1, the method further comprising:

implementing, by the secure interface control, a create central processing unit (CPU) instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control and qualified with the associated secure-guest-domain, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

8. The method of claim 1, wherein the donated storage comprises all secure interface control storage donated by the untrusted entity.

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

receiving, by a secure interface control of a system, an initialization instruction from an untrusted entity of the system to set donated storage from the untrusted entity as secure, wherein the untrusted entity facilitates deploying one or more virtual machines on the system, and the secure interface control facilitates the untrusted entity in providing one or more services to the one or more virtual machines;

implementing, by the secure interface control, the initialization instruction through assigning a portion of the donated storage as zone-specific storage and tagging the zone

specific storage with a unique-secure domain for secure control that prevents access by the untrusted entity and the one or more virtual machines; and

assigning, by the secure interface control, secure guest-domain-specific storage and tagging the secure-guest-domain-specific storage as belonging to the secure interface control and qualified with an associated secure-guest-domain, wherein the secure-guest-domain provides secure access to one of the one or more virtual machines and prevents access from the untrusted entity.

10. The computer program product of claim 9, wherein the implementing of the initialization instruction causes the secure interface control to verify the donated storage as non-secure and set the donated storage as secure storage.

11. The computer program product of claim 9, wherein the implementing of the initialization instruction causes the secure interface control to assign a portion of the donated storage to be defined as absolute storage and tag this portion of the donated storage as having no associated virtual address.

12. The computer program product of claim 9, wherein the implementing of the initialization instruction causes the secure interface control to assign a portion of the donated storage to be defined as virtual storage and tag this portion of the donated storage with an associated virtual address.

13. The computer program product of claim 9, wherein the donated storage is registered to the secure interface control and the donated storage is marked as secure.

14. The computer program product of claim 9, the method further comprising:

implementing, by the secure interface control, a create configuration instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

15. The computer program product of claim 9, the method further comprising:

implementing, by the secure interface control, a create central processing unit (CPU) instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control and qualified with the associated secure-guest-domain, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

16. A system comprising:

a memory;

a processing unit; and

a secure interface control interfaced with the processing unit and the memory, the secure interface control in communication with an untrusted entity and configured to perform operations comprising:

receiving an initialization instruction from the untrusted entity to set donated storage from the untrusted entity as secure, wherein the untrusted entity facilitates deploying one or more virtual machines on the system, and the secure interface control facilitates the untrusted entity in providing one or more services to the one or more virtual machines;

implementing the initialization instruction through assigning a portion of the donated storage as zone-specific storage and tagging the zone-specific storage with a unique-secure domain for secure control that prevents access by the untrusted entity and the one or more virtual machines; and

assigning secure guest-domain-specific storage and tagging the secure-guest-domain-specific storage as belonging to the secure interface control and qualified with an associated secure-guest-domain, wherein the secure-guest-domain provides secure access to one of the one or more virtual machines and prevents access from the untrusted entity.

17. The system of claim 16, wherein the implementing of the initialization instruction causes the secure interface control to verify the donated storage as non-secure and set the donated storage as secure storage.

18. The system of claim 16, wherein the implementing of the initialization instruction causes the secure interface control to assign a portion of the donated storage to be defined as absolute storage and tag this portion of the donated storage as having no associated virtual address.

19. The system of claim 16, wherein the secure interface control is configured to perform operations comprising:

implementing a create configuration instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

20. The system of claim 16, wherein the secure interface control is configured to perform operations comprising:

implementing a create central processing unit (CPU) instruction that registers the donated storage to the secure interface control, marks the donated storage as secure, and causes the secure interface control to tag the donated storage as belonging to the secure interface control and qualified with the associated secure-guest-domain, the implementing of the create configuration instruction being responsive to a second instruction call issued from the untrusted entity.

21. A method comprising:

implementing, by a secure interface control in communication with an untrusted entity in a system, an initialize secure interface control instruction that registers donated storage to the secure interface control and marks the donated storage as secure, the implementing of the initialize secure interface control instruction being responsive to a first instruction call issued from the untrusted entity, wherein the untrusted entity facilitates deploying one or more virtual machines on the system, and the secure interface control facilitates the untrusted entity in providing one or more services to the one or more virtual machines;

implementing, by the secure interface control, a create secure configuration instruction that registers the donated storage to the secure interface control and marks the

donated storage as secure, the implementing of the create secure configuration instruction being responsive to a second instruction call issued from the untrusted entity to provide secure access to one of the one or more virtual machines and prevent access by the untrusted entity; and

implementing, by the secure interface control, a create secure central processing unit (CPU) instruction that registers the donated storage to the secure interface control and marks the donated storage as secure, the implementing of the create secure CPU instruction being responsive to a third instruction call issued from the untrusted entity to create one or more virtual CPUs for one of the one or more virtual machines and prevent access by the untrusted entity.

22. The method of claim 21, wherein the implementing of the initialize secure interface control instruction causes the secure interface control to assign the donated storage as zone-specific storage and tag the zone-specific storage with a unique-secure domain,

wherein the implementing of the create secure configuration instruction causes the secure interface control to assign donated base-secure-configuration and variable-secure-configuration storage as secure guest-domain-specific storage and tag the secure guest-domain-specific storage as belonging to the secure interface control and qualified with an associated secure-guest-domain, or

wherein the implementing of the create secure CPU instruction causes the secure interface control to assign donated base-secure-CPU storage as secure guest-domain-specific storage and tag the secure guest-domain-specific storage as belonging to the secure interface control and qualified with the associated secure-guest-domain.

23. The method of claim 22, wherein the donated zone-specific storage, the base-secure-configuration storage, or the base-CPU storage is defined as absolute storage and tagged as having no associated virtual address, and

wherein the donated variable-secure-configuration storage is defined as virtual storage and tagged with the associated virtual address.

24. The method of claim 21, wherein the implementing of the initialize secure interface control, the create secure configuration, or the create secure CPU instructions cause the

secure interface control to verify donated storage as non-secure and set the donated storage as secure.

25. The method of claim 21, wherein the donated storage comprises all secure interface control storage donated by the untrusted entity.