CLAIMS

1. A method comprising:

receiving, by a communication interface (1580) of a secure interface control (1530) executing between the secure interface control (1530) of a computer (10) and hardware (1501) of the computer (10), an instruction from a calling entity to perform a secure interface control function;

determining, by the communication interface (1580), whether the instruction is a millicoded instruction;

entering, by the communication interface (1580), a millimode comprising enabling the secure interface control (1530) to engage millicode (1570) of the hardware (1501) through the communication interface (1580) based on the instruction being the millicoded instruction; and

executing, by the millicode (1570), the instruction, wherein:

during execution of the instruction, the hardware (1501) of the computer (10) maintains a state of the calling entity, while it is running, independent of a state of the millicode (1750); and

the secure interface control (1530) includes a hardware mechanism that prevents storage locations assigned to secure entities (1541, 1542) from being accessed by other secure entities (1541, 1542) or by unsecured entities (1521, 1522).

2. The method of claim 1, wherein the instruction is executed by the hardware (1501) of the computer (10) based on the instruction not being the millicoded instruction.

3. The method of claim 1 or 2, wherein the communication interface (1580) exits the millimode after the instruction is executed by the millicode (1570).

4. The method of one of claims 1 to 3, wherein the calling entity is an unsecured entity (1521, 1522) or a secured entity (1541, 1542).

5. The method of claim 4, wherein the unsecured entity (1521, 1522) comprises a hypervisor (1521, 1522), the secured entity (1541, 1542) comprises a secured guest, and the instruction comprises an architected instruction.

6. The method of one of claims 1 to 5, wherein the millicode (1570) utilizes enhancements of the communication interface (1580) to access secure storage associated with the instruction in a secure execution context.

7. The method of one of claims 1 to 6, wherein the millicode (1570) is an extension of the hardware (1501) that performs functions of the secure interface control (1530) upon executing the instruction.

8. The method of one of claims 1 to 7, wherein the millicode (1570), acting as the secure interface control (1530), is dispatching a secure entity (1541, 1542) and sets an indication that a secure entity (1541, 1542) is running and loads a secure guest state into the hardware (1501).

9. The method of claim 8, wherein the hardware (1501) uses the secure guest state to execute security checks while a secure guest domain associated with the secure entity (1541, 1542) is running.

10. A computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable a computer (10) to cause operations comprising:

receiving, by a communication interface (1580) of a secure interface control (1530) executing between the secure interface control (1530) of a computer (10) and hardware (1501) of the computer (10), an instruction from a calling entity to perform a secure interface control function;

determining, by the communication interface (1580), whether the instruction is a millicoded instruction;

entering, by the communication interface (1580), a millimode comprising enabling the secure interface control (1530) to engage millicode (1570) of the hardware (1501) through the communication interface (1580) based on the instruction being the millicoded instruction; and

executing, by the millicode (1570), the instruction, wherein:

during execution of the instruction, the hardware (1501) of the computer (10) maintains a state of the calling entity, while it is running, independent of a state of the millicode (1750); and

the secure interface control (1530) includes a hardware mechanism that prevents storage locations assigned to secure entities (1541, 1542) from being accessed by other secure entities (1541, 1542) or by unsecured entities (1521, 1522).

11. The computer program product of claim 10, wherein the instruction is executed by the hardware (1501) of the computer (10) based on the instruction not being the millicoded instruction.

12. The computer program product of claim 10 or 11, wherein the communication interface (1580) exits the millimode after the instruction is executed by the millicode (1570).

13. The computer program product of one of claims 10 to 12, wherein the calling entity is an unsecured entity (1521, 1522) or a secured entity (1541, 1542).

14. The computer program product of claim 13, wherein the unsecured entity (1521, 1522) comprises a hypervisor (1521, 1522), the secured entity (1541, 1542) comprises a secured guest, and the instruction comprises an architected instruction.

15. The computer program product of one of claims 10 to 14, wherein the millicode (1570) utilizes enhancements of the communication interface (1580) to access secure storage associated with the instruction in a secure execution context.

16. The computer program product of one of claims 10 to 15, wherein the millicode (1570) is an extension of the hardware (1501) that performs functions of the secure interface control (1530) upon executing the instruction.

17. The computer program product of one of claims 10 to 16, wherein the millicode (1570), acting as the secure interface control (1530), is dispatching a secure entity (1541, 1542) and sets an indication that a secure entity (1541, 1542) is running and loads a secure guest state into the hardware (1501).

18. The computer program product of claim 17, wherein the hardware (1501) uses the secure guest state to execute security checks while a secure guest domain associated with the secure entity (1541, 1542) is running.

19. A system comprising:

hardware (1501) comprising a millicode (1570);

a secure interface control (1530);

a communication interface (1580) of the secure interface control (1530) executing between the secure interface control (1530) and the hardware (1501);

wherein the system is executable to cause operations comprising:

receiving, by the communication interface (1580), an instruction from a calling entity to perform a secure interface control function;

determining, by the communication interface (1580), whether the instruction is a millicoded instruction;

entering, by the communication interface (1580), a millimode comprising enabling the secure interface control (1530) to engage millicode (1570) of the hardware (1501) through the communication interface (1580) based on the instruction being the millicoded instruction; and

executing, by the millicode (1570), the instruction, wherein:

during execution of the instruction, the hardware (1501) of the computer (10) maintains a state of the calling entity, while it is running, independent of a state of the millicode (1570); and

the secure interface control (1530) includes a hardware mechanism that prevents storage locations assigned to secure entities (1541, 1542) from being accessed by other secure entities (1541, 1542) or by unsecured entities (1521, 1522).

20. The system of claim 19, wherein the instruction is executed by the hardware (1501) of the computer (10) based on the instruction not being the millicoded instruction.

21. The system of claim 19 or 20, wherein the communication interface (1580) exits the millimode after the instruction is executed by the millicode (1570).

22. The system of one of claims 19 to 21, wherein the calling entity is an unsecured entity (1521, 1522) or a secured entity (1541, 1542).

23. The system of claim 22, wherein the unsecured entity (1521, 1522) comprises a hypervisor (1521, 1522), the secured entity (1541, 1542) comprises a secured guest, and the instruction comprises an architected instruction.

24. The system of one of claims 19 to 23, wherein the millicode (1570) utilizes enhancements of the communication interface (1580) to access secure storage associated with the instruction in a secure execution context.

25. The system of one of claims 19 to 24, wherein the millicode (1570) is an extension of the hardware (1501) that performs functions of the secure interface control (1530) upon executing the instruction.