CLAIMS

1. A computer system comprising:
a first partition and a second partition;
the first partition comprising:
a first CPU, and
a first memory module, comprising:
at least one memory address range for program code, wherein the program code comprises computer-executable code, and which is configured by hardware circuitry;
at least one memory address range for other data, comprising data read from the second partition; and
wherein the first CPU is hardware-configured to execute only the computer-executable code in the memory address range for program code;
the second partition comprising:
a second CPU,
a second memory module, and
at least one communication module configured to couple to a network;
wherein the first CPU can read from the second memory module only into the at least one memory address range for other data;
wherein the first CPU can write to the second memory module; and
wherein the second CPU is restricted from accessing the first memory module.

2. The computer system of claim 1, wherein the memory addressing structure comprises:
a first memory unit for the at least one memory address range for program code; and
a second memory unit for the at least one memory address range for other data.

3. The computer system of claim 1, wherein the hardware circuitry mapping the memory addressing structure for program code comprises at least one field-programmable gate array.

4. The computer system of claim 1, wherein the at least one memory address range for other data comprises:
at least one memory address range for data read from the second partition, and
at least one memory address range for other first partition data.

5. The computer system of claim 1, wherein the memory addressing structure comprises:
a first memory unit for the at least one memory address range for program code;
a second memory unit for data read from the second partition; and
a third memory unit for other first partition data.

6. The computer system of claim 1, comprising at least one external physical switch which can be turned on or off, wherein the first CPU can modify data stored in the at least one address range for program code only when the external physical switch is on.

7. The computer system of claim 1, comprising at least one external physical switch which can be turned on or off,
wherein the first CPU can modify data stored in the at least one memory address range for program code only when the external physical switch is on; and
wherein, while the at least one external physical switch is on, the ability of the first CPU to access the second CPU and the second memory module is disabled.

8. The computer system of claim 1, wherein a hardware feature, utilizing an external device connected directly to the first partition, is configured to enable a user to command the first CPU to take control of one or more input/output devices connected to the second partition.

9. The computer system of claim 1, wherein the at least one address range for program code comprises an operating system.

10. The computer system of claim 1, comprising at least one data store.

11. The computer system of claim 1, wherein a plurality of input/output devices are coupled to at least one I/O module.

12. The computer system of claim 1, further comprising a chip comprising the first partition and second partition.

13. The computer system of claim 1, further comprising a first chip comprising the first partition and a second chip comprising the second partition.

14. The computer system of claim 1,

wherein the ability of the first CPU to access the second memory module and the second CPU, is implemented by hardware circuitry;

wherein the first CPU can read from the second partition into only the at least one memory address range for other data; and

wherein the restriction on the second CPU from accessing the first CPU or the first memory module is implemented by hardware circuitry.

15. The computer system of claim 1, further comprising a bus,

wherein the first partition is interconnected to the second partition through the bus;

wherein the first partition is configured to execute a pull command through the bus to read data from the second partition and write the data only to the at least one memory address range applicable for other data; and

wherein the first partition is configured to execute a push command through the bus to write data to the second partition.

16. The computer system of claim 1, comprising a hardware unit,

wherein the unit is configured to be connected through the Internet only to one or more predefined services, to download new critical applications or update existing ones;

wherein the unit is configured to connect to the first partition or write the update data onto a nonvolatile memory; and

wherein the first partition is configured to accept data from the unit or the nonvolatile memory only when a hardware switch is on.

17. The computer system of claim 1, comprising a hardware unit built into the system,
wherein the unit comprises fixed hardware or firmware configured to connect through the Internet only to one or more predefined services; and
wherein the first partition is configured to accept data from the unit only when a hardware switch is on.

18. The computer system of claim 1, connected to a device able to communicate over a network, such as the internet or through local wireless communication including but not limited to Bluetooth and RFID transmission, wherein the device or computer system is prepared before distribution by manufacturer with a security key or keys placed into protected memory.

19. The computer system of claim 1, configured to comprise more than one first partition, or more than one second partition, or more than one first and second partitions,
wherein the CPU of each second partition is hardware-restricted from accessing the CPU or memory module of each first partition.

20. The computer system of claim 1, wherein:
the first partition comprises one or more virtual sub-partitions; and
the second partition comprises one or more virtual sub-partitions.

21. A computer system comprising:
a first virtual partition family and a second virtual partition family;
the first virtual partition family comprising:
at least one partition,
at least one CPU, and
at least one memory module comprising:

at least one address range for program code, wherein the program code comprises computer-executable code, wherein the at least one address range for program code is configured as read-only in the normal operation state; and

at least one memory address range for other data, comprising data read from the second virtual partition family;

wherein the at least one CPU of the first virtual partition family is configured to execute only the computer-executable code stored in the at least one address range for program code;

the second virtual partition family comprising:

at least one partition,

at least one CPU,

at least one memory module, and

at least one communication module capable of coupling to a network;

wherein the at least one CPU of the first virtual partition family is configured to be able to access the at least one memory module of the second virtual partition family; and

wherein the at least one CPU of the second virtual partition family is configured to be unable to access the first virtual partition family.

22. The computer system of claim 21, comprising a hardware feature, utilizing at least one device connected to the computer, and which can be turned on or off, wherein the at least one CPU of the first virtual partition family cannot modify data in the at least one address range for program code, unless the hardware device is on.

23. The computer system of claim 21, comprising:

a hardware feature, comprising at least one device connected to the computer, and comprising an on position and an off position,

wherein the at least one CPU of the first virtual partition family cannot modify data in the at least one address range for program code unless the hardware device is in the on position; and

wherein, while the at least one hardware device is in the on position, the ability of the at least one CPU of the first virtual partition family to access the second virtual partition family is disabled.

24. The computer system of claim 21, wherein:

a hardware device is placed between a server bank hosting virtual servers and the router used to connect to a network such as the internet,

wherein the device directs all traffic between the partitions, or between external units or computers connected to the partitions, so that no code or data may be written to the first virtual partition except as initiated by the first virtual partition or when permitted by the hardware switch; and

wherein the device itself may be configured to direct traffic down its three separate pathways (read and write, read only, and no connection/ rejection of request) only when its configuration switch is in the on position.

25. The computer system of claim 21, comprising at least one hardware device connected to the computer, wherein the at least one hardware device can be turned on or off, wherein the virtual configuration of the first virtual partition family cannot be modified unless the at least one hardware device is on.

26. A computer system comprising:

a first computer and a second computer;

the first computer, comprising:

a CPU, and

a memory module, comprising:

at least one memory address range for program code, wherein the program code comprises computer-executable code, and which is configured by hardware circuitry;

at least one memory address range for other data, comprising data read from the second computer; and

wherein the CPU is hardware-configured to execute only the computer-executable code in the memory address range for program code;

the second computer, comprising:

a CPU, and

at least one communication module configured to couple to a network;

a bus,

wherein the first computer and the second computer are interconnected only through the bus;

wherein the bus is configured for the first computer to execute a pull command through the bus to read data from the second computer and write the data only to the at least one memory address range applicable to data read from the second computer;

wherein the bus is configured for the first computer to execute a push command through the bus to send data to the second computer;

wherein the bus cannot accept a push command from the second computer;

wherein the bus cannot accept a pull command from the second computer; and

wherein the hardware circuitry of the bus does not permit the second computer to access the memory module of the first computer.

27. The computer system of claim 26, wherein the memory module comprises:

a first memory unit for the at least one memory address range for program code; and

a second memory unit for the at least one memory address range for other data.

28. The computer system of claim 26, wherein the hardware circuitry mapping the memory addressing structure for program code comprises at least one field-programmable gate array.

29. The computer system of claim 26, wherein the at least one memory address range for other data comprises:

at least one memory address range for data read from the second computer, and

at least one memory address range for other first computer data.

30. The computer system of claim 26, wherein the memory module comprises:

a first memory unit for the at least one memory address range for program code;

a second memory unit for data read from the second computer; and
a third memory unit for other first computer data.

31. The computer system of claim 26, comprising at least one external physical switch which can be turned on or off, wherein the CPU of the first computer can modify data stored in the at least one memory address range for program code only when the external physical switch is on.

32. The computer system of claim 26, wherein the at least one address range for program code comprises an operating system.

33. The computer system of claim 26, comprising at least one data store.

34. The computer system of claim 26,
wherein the first computer comprises at least one input/output module; and
wherein a plurality of input/output devices are coupled to the at least one input/output module.