IN THE CLAIMS:

1. (Four Times Amended) A method of operating a computer system capable of exchanging data across a network of one or more computers and having at least a first and second electronic data processor capable of executing instructions using a common operating system, comprising[the steps of]:

executing a first web browser process~~instructions~~, capable of accessing data of a website via the network, in a first logical process within the common operating system using the first electronic data processor, wherein the first logical process is capable of accessing data contained in a first memory space[and a second memory space];

executing a second web browser process~~instructions~~ in a second logical process within the common operating system using the second electronic data processor, wherein the second logical process is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

displaying[, in a windowed format on a display terminal,] data from the first logical process and the second logical process, wherein a video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser~~logical~~ process.

2. (Twice Amended) The method of claim 1 wherein the[first memory space and the] second memory space [comprise separate regions of a common memory space is]comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

3. (Twice Amended) The method of claim 1 wherein the first logical process is capable of accessing data contained in the second memory space~~second logical process is selected from the group consisting of:~~

~~an electronic mail process, an instant messaging process, an internet browser process, an interactive gaming process, a virtual private network (VPN) process, and a reader application process~~.

4. (Original) The method of claim 1 wherein the first logical process receives user interface data, and passes the user interface data to the second logical process.

5. (Original) The method of claim 1 wherein the first and second electronic data processors are part of a multi-core electronic data processor.

6. (Twice Amended) The method of claim 1 and further comprising[the step of] restoring at least one corrupted data file[residing on the second memory space] from [an]a protected image[residing on the first memory space].

7. (Amended) The method of claim 1 and further comprising[the step of] automatically deleting at least one data file residing on the second memory space when the second logical process is terminated.

8. (Amended) The method of claim 1 and further comprising[the steps of]:

encrypting data with the first logical process;

transferring the encrypted data from the first logical process to the second logical process; and

transferring the encrypted data from the second logical process to the network interface device.

9. (Amended) The method of claim 8 and further comprising[the steps of]:

decrypting the data with the network interface device; and

transferring the decrypted data from the network interface device to the network.

10. (Four Times Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers via a network interface device, comprising:

a first electronic data processor capable of executing a first web browser process~~instructions~~ using the common operating system and communicatively coupled to a first memory space[and a second memory space], the first web browser process capable of accessing data of a website via the network;

a second electronic data processor capable of executing a second web browser process~~instructions~~ using the common operating system and communicatively coupled to [the]a second memory space[and a network interface device, wherein the second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device]; and

a video processor adapted to combine video data from the first and second electronic data processors and transmit the combined video data to a display[terminal for displaying the

combines video data in a windowed format];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from corruption by a malware process downloaded from the network and executing as part of the second web browser process~~on the second electronic data processor~~.

11. (Twice Amended) The computer system of claim 10 wherein the[first memory space and the] second memory space[comprise separate regions of a common memory space is] comprises memory selected from the group consisting of:

a memory zone within a physical memory common to the first memory space;

a partition on a memory device;

random access memory (RAM); and

both volatile and nonvolatile memory.

12. (Original) The computer system of claim 10 wherein the first and second electronic data processors are part of a dual processor computer system.

13. (Original) The computer system of claim 10 wherein the second electronic data processor and the video processor are co-located on a circuit card, the circuit card being communicatively coupled to the first electronic data processor.

14. (Original) The computer system of claim 10 wherein the computer system is configured such that the first electronic data processor is protected from executing instructions initiated by a malware process downloaded from the network and executing on the second electronic data processor.

15. (Four Times Amended) A multi-processor computer system using a common operating system capable of exchanging data across a network of one or more computers,

comprising:

at least a first and second electronic data processor capable of executing instructions using the common operating system;

at least a first and second memory space; and

a video processor;

wherein the first and second electronic data processors, first and second memory space, and video processor are configured to:[for performing the steps of;]

[executing]execute a first web browser process~~instructions~~, capable of accessing data of a website via the network, in a first logical process with the first electronic data processor, wherein the first logical process is executing within the common operating system and is capable of accessing data contained in the first memory space;

[executing]execute a second web browser process~~instructions~~ in a second logical process with the second electronic data processor, wherein the second logical process is executing within the common operating system and is capable of accessing data contained in the second memory space[, the second logical process being further capable of exchanging data across a network of one or more computers]; and

[displaying, in a windowed format on a display terminal,]display data from the first logical process and the second logical process, wherein the video processor is adapted to combine data from the first and second logical processes and transmit the combined data to [the]a display[terminal];

wherein the computer system is configured such that the second electronic data processor is operating in a protected mode and data residing on the first memory space is protected from

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.