(19) **United States**

(12) **Reissued Patent** (10) Patent Number: **US RE43,528 E**

Rozman et al. (45) Date of Reissued Patent: *Jul. 17, 2012

(54) **SYSTEM AND METHOD FOR PROTECTING A COMPUTER SYSTEM FROM MALICIOUS SOFTWARE**

(76) Inventors: **Allen F. Rozman**, Garland, TX (US);
Alfonso J. Cioffi, Murphy, TX (US)

(*) Notice: This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/720,147**

(22) Filed: **Mar. 9, 2010**

Related U.S. Patent Documents

Reissue of:
(64) Patent No.: **7,484,247**
Issued: **Jan. 27, 2009**
Appl. No.: **10/913,609**
Filed: **Aug. 7, 2004**

(51) **Int. Cl.**
H04L 29/06 (2006.01)
G06F 11/00 (2006.01)
G06F 12/14 (2006.01)
G06F 12/16 (2006.01)
G08B 23/00 (2006.01)

(52) **U.S. Cl.** **713/152**; 713/151; 726/22; 726/23; 726/24

(58) **Field of Classification Search** 726/22–24; 713/152, 151; 709/225
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,890,098	A	12/1989	Dawes et al.
5,280,579	A	1/1994	Nye
5,502,808	A	3/1996	Goddard et al.
5,555,364	A	9/1996	Goldstein
5,564,051	A *	10/1996	Halliwell et al. 1/1
5,666,030	A	9/1997	Parson
5,673,403	A *	9/1997	Brown et al. 715/744
5,751,979	A *	5/1998	McCrory 715/803
5,826,013	A	10/1998	Nachenberg
5,918,039	A	6/1999	Buswell et al.
5,974,549	A *	10/1999	Golan 726/23
5,978,917	A	11/1999	Chi
5,995,103	A	11/1999	Ashe
6,091,412	A	7/2000	Simonoff et al.
6,108,715	A	8/2000	Leach et al.
6,134,661	A	10/2000	Topp
6,167,522	A	12/2000	Lee et al.
6,183,366	B1	2/2001	Goldberg et al.

(Continued)

OTHER PUBLICATIONS

Architecture of Virtual Machines by R. P. Goldberg, Honeywell Information Systems, Inc. and Harvard University presented at the AFIPS National Computer Conference, New York, New York, Jun. 4-8, 1973.

(Continued)

Primary Examiner — Christian LaForgia
(74) *Attorney, Agent, or Firm* — Slater & Matsil, L.L.P.

(57) **ABSTRACT**

In a computer system, a first electronic data processor is communicatively coupled to a first memory space and a second memory space. A second electronic data processor is communicatively coupled the second memory space and to a network interface device. The second electronic data processor is capable of exchanging data across a network of one or more computers via the network interface device. A video processor is 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 combined video data in a windowed format. The computer system is configured such that a malware program downloaded from the network and executing on the second electronic data processor is incapable of initiating access to the first memory space.

73 Claims, 11 Drawing Sheets
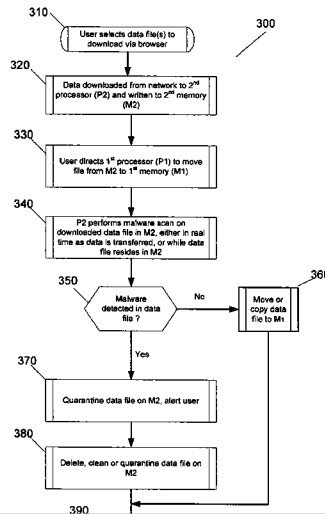
U.S. PATENT DOCUMENTS

6,192,477	B1 *	2/2001	Corthell	726/11
6,199,181	B1 *	3/2001	Rechef et al.	714/38
6,216,112	B1	4/2001	Fuller et al.	
6,275,938	B1	8/2001	Bond et al.	
6,285,987	B1	9/2001	Roth et al.	
6,321,337	B1	11/2001	Reshef et al.	
6,351,816	B1	2/2002	Mueller et al.	
6,385,721	B1 *	5/2002	Puckette	713/2
6,397,242	B1	5/2002	Devine et al.	
6,401,134	B1	6/2002	Razavi et al.	
6,433,794	B1	8/2002	Beadle et al.	
6,438,600	B1	8/2002	Greenfield et al.	
6,480,198	B2	11/2002	Kang	
6,492,995	B1	12/2002	Atkin et al.	
6,505,300	B2	1/2003	Chan et al.	
6,507,904	B1	1/2003	Ellison et al.	
6,507,948	B1	1/2003	Curtis et al.	
6,546,554	B1	4/2003	Schmidt et al.	
6,553,377	B1	4/2003	Eschelbeck et al.	
6,578,140	B1 *	6/2003	Policard	713/1
6,581,162	B1	6/2003	Angelo et al.	
6,633,963	B1	10/2003	Ellison et al.	
6,658,573	B1	12/2003	Bischof	
6,663,000	B1	12/2003	Muttik et al.	
6,678,712	B1 *	1/2004	McLaren et al.	718/100
6,678,825	B1	1/2004	Ellison et al.	
6,691,230	B1	2/2004	Bardon	
6,735,700	B1	5/2004	Flint et al.	
6,754,815	B1 *	6/2004	Ellison et al.	713/1
6,756,236	B2	6/2004	Ford et al.	
6,757,685	B2	6/2004	Raffaele et al.	
6,772,345	B1	8/2004	Shetty	
6,804,780	B1	10/2004	Touboul	
6,836,885	B1	12/2004	Buswell et al.	
6,871,348	B1 *	3/2005	Cooper	719/310
6,873,988	B2	3/2005	Herrmann et al.	
6,880,110	B2	4/2005	Largman et al.	
6,990,630	B2	1/2006	Landsman et al.	
6,996,828	B1 *	2/2006	Kimura et al.	719/319
7,013,484	B1 *	3/2006	Ellison et al.	726/26
7,024,555	B2 *	4/2006	Kozuch et al.	726/22
7,024,581	B1 *	4/2006	Wang et al.	714/2
7,039,801	B2 *	5/2006	Narin	713/152
7,062,672	B2	6/2006	Owhadi et al.	
7,082,615	B1 *	7/2006	Ellison et al.	726/26
7,085,928	B1	8/2006	Schmid et al.	
7,096,381	B2	8/2006	Largman et al.	
7,139,890	B2	11/2006	Moran et al.	
7,146,305	B2 *	12/2006	van der Made	703/22
7,146,640	B2 *	12/2006	Goodman et al.	726/16
7,181,768	B1	2/2007	Ghosh et al.	
7,191,469	B2	3/2007	Erlingsson	
7,246,374	B1	7/2007	Simon et al.	
7,260,839	B1 *	8/2007	Karasaki	726/11
7,284,274	B1	10/2007	Walls et al.	
7,367,057	B2 *	4/2008	Das et al.	726/24
7,373,505	B2	5/2008	Seltzer et al.	
7,401,230	B2	7/2008	Campbell et al.	
7,421,689	B2	9/2008	Ross et al.	
7,444,412	B2	10/2008	Owhadi	
7,484,247	B2 *	1/2009	Rozman et al.	726/34
7,565,522	B2	7/2009	Sastry et al.	
7,577,871	B2	8/2009	Largman et al.	
7,596,694	B1	9/2009	Karp et al.	
7,650,493	B2 *	1/2010	Narin	713/152
7,657,419	B2 *	2/2010	van der Made	703/22
7,676,842	B2	3/2010	Carmona et al.	
7,694,328	B2	4/2010	Joshi et al.	
7,730,318	B2	6/2010	Kurien et al.	
7,818,808	B1 *	10/2010	Neiger et al.	726/26
7,849,310	B2 *	12/2010	Watt et al.	713/164
7,854,008	B1 *	12/2010	Huang et al.	726/24
2002/0002673	A1 *	1/2002	Narin	713/152
2002/0052809	A1	5/2002	Toedtli	
2002/0066016	A1	5/2002	Riordan	
2002/0174349	A1	11/2002	Wolff et al.	
2003/0131152	A1	7/2003	Erlingsson	
2003/0177397	A1	9/2003	Samman	
2003/0221114	A1 *	11/2003	Hino et al.	713/189
2004/0006706	A1 *	1/2004	Erlingsson	713/200
2004/0006715	A1	1/2004	Skrepetos	
2004/0034794	A1	2/2004	Mayer et al.	
2004/0039944	A1 *	2/2004	Karasaki	713/201
2004/0054588	A1	3/2004	Jacobs et al.	
2004/0199763	A1	10/2004	Freund	
2004/0230794	A1 *	11/2004	England et al.	713/164
2004/0267929	A1 *	12/2004	Xie	709/225
2005/0005153	A1 *	1/2005	Das et al.	713/200
2005/0091661	A1 *	4/2005	Kurien et al.	719/310
2005/0149726	A1 *	7/2005	Joshi et al.	713/164
2005/0198692	A1 *	9/2005	Zurko et al.	726/24
2005/0240810	A1	10/2005	Safford et al.	
2006/0004667	A1	1/2006	Neil	

OTHER PUBLICATIONS

The Duality of Memory and Communication in the Implementation of a Multiprocessor Operating System by Michael Young, Avadis Tevanian, Richard Rasheed, David Golub, Jeffery Eppinger, Jonathan Crew, William Bolosky, David Black and Robert Baron, Computer Science Department Carnegie-Mellon University Appeared in Proceedings of the 11th Operating Systems Principles, Nov. 1987.

Application-Controlled Physical Memory using External Page-Cache Management by Keiran Harty and David R. Cheriton, Computer Science Department, Stanford University, 1992.

Efficient Software-Based Fault Isolation by Robert Wahbe, Steven Lucco, Thomas Anderson, Susan Graham, Computer Science Division University of California, Berkeley, SIGOPS 1993.

Tron: Process-Specific File Protection for the UNIX Operating System by Andrew Berman, Virgil Bourassa, Erik Selberg, Department of Computer Science and Engineering, University of Washington, Jan. 23, 1995.

A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker) by Ian Goldberg, David Wagner, Randi Thomas, and Eric Brewer, Computer Science Division, University of California, Berkeley, Sixth USENIX UNIX Security Symposium San Jose, California, Jul. 1996.

Building Systems that Flexibly Control Downloaded Executable Context by Trent Jaeger and Atul Prakash, Software Systems Research Lab, University of Michigan and Aviel D. Rubin, Security Research Group, Bellcore Sixth USENIX UNIX Security Symposium San Jose, California, Jul. 1996.

Java Security: From HotJava to Netscape and Beyond by Drew Dean, Edward W. Felten, Dan S. Wallach Department of Computer Science, Princeton University, Princeton, NJ 08544 1996 IEEE Symposium on Security and Privacy, Oakland, CA, May 6-8, 1996.

ChakraVyuha (CV) : A Sandbox Operating SystemEnvironment for Controlled Execution of Alien Code by Asit Dan, Ajay Mohindra, Rajiv Ramaswami, and Dinkar Sitaram IBM Research Division T.J. Watson Research Center Yorktown Heights, New York RC 20742 (Feb. 20, 1997) Computer Science IBM Research Report Limited Distribution.

Vulnerability of Secure Web Browsers by Flavio De Paoli, Andre Dos Santos, Richard Kemmerer Reliable Software Group Computer Science Department, University of California, Santa Barbara, 1997.

Security of Web Browser Scripting Languages: Vulnerabilities, Attacks, and Remedies by Vinod Anupam and Alain Mayer, Bell Laboratories, Lucent Technologies 7th USENIX Security Symposium San Antonio, Texas, Jan. 26-29, 1998.

"Virtual Memory in Contemporary Microprocessors" by Bruce Jacob University of Maryland and Trevor Mudge University of Michigan, IEEE Micro Jul.-Aug. 1998.

"Flexible Control of Downloaded Executable Content" by Trent Jaeger and Jochen Liedtke and Nayeem Islam, IBM Thomas J. Watson Research Center, and Atul Prakash University of Michigan,

"J2ME Building Blocks for Mobile Devices: White Paper on KVM and the Connected", Limited Device Configuration Sun Microsystems May 19, 2000.

"User-level Resource-constrained Sandboxing" by Fangzhe Chang, Ayal Itzkovitz, and Vijay Karamcheti Department of Computer Science, Courant Institute of Mathematical Sciences, New York University USENIX Windows System Symposium, Aug. 2000.

"Verifying the EROS Confinement Mechanism" by Jonathan S. Shapiro and San Weber IBM T.J. Watson Research Center 0-7695-0665-8/00 2000 IEEE.

"WindowBox: A Simple Security Model for the Connected Desktop" by Dirk Balfanz, Princeton University and Daniel R. Simon, Microsoft Research, 2000.

"Building a Secure Web Browser" by Sotiris Ioannidis, University of Pennsylvania, and Steven M. Bellovin, At&T Labs Research 2001 USENIX Annual Technical Conference Boston, Massachusetts, USA Jun. 25-30, 2001.

"Virtualizing I/O Devices on VMware Workstation's Hosted Virtual Machine Monitor" by Jeremy Sugerman, Ganesh Venkitachalam and Beng-Hong Lim, VMware, Inc. 3145 Porter Dr, Palo Alto, CA 943042001 USENIX Annual Technical Conference Boston, Massachusetts, USA Jun. 25-30, 2001.

"When Virtual Is Better Than Real" by Peter M. Chen and Brian D. Noble, Department of Electrical Engineering and Computer Science University of Michigan 2001.

"A Flexible Containment Mechanism for Executing Untrusted Code" by David Peterson, Matt Bishop, and Raju Pandey, Department of Computer Science University of California, Davis USENIX Security Symposium San Francisco, California, USA Aug. 5-9, 2002.

"ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay" by George W. Dunlap, Samuel T. King, Sukru Cinar, Murtaza A. Basrai, Peter M. Chen, Department of Electrical Engineering and Computer Science, University of Michigan Proceedings of the 2002 Symposium on Operating Systems Design and Implementation (OSDI).

"Trusted Paths for Browsers: an Open-Source Solution to Web Spoofing" by Zishuang (Eileen) Ye and Sean Smith, Department of Computer Science Dartmouth College, Technical Report TR2002-418 Feb. 4, 2002.

"User Interaction Design for Secure Systems" by Ka-Ping Yee http://zesty.ca/sid/ 2002.

BAA-00-06-SNK Focused Research Topic 5 by Marc Stiegler and Mark Miller Report Name: "A Capability Based Client: The DarpaBrowser" Jun. 26, 2002.

"A Virtual Machine Introspection Based Architecture for Intrusion Detection" by Tal Garfinkel and Mendel Rosenblum, Computer Science Department, Stanford University 2003.

"Terra: A Virtual Machine-Based Platform for Trusted Computing" by Tal Garfinkel, Ben Pfaff, Jim Chow, Dan Boneh and Mendel Rosenblum, Computer Science Department, Stanford University SOSP'03, Oct. 19-22, 2003, Bolton Landing, New York, USA.

Microsoft® Virtual PC 2004 Technical Overview by Jerry Honeycutt Published Nov. 2003 http://download.microsoft.com/download/c/f/b/cfb100a7-463d-4b86-ad62-064397178b4f/Virtual_PC_Technical_Overview.doc.

"Xen and the Art of Virtualization" by Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebaurey,

Ian Pratt, Andrew Warfield University of Cambridge Computer Laboratory 15 JJ Thomson Avenue, Cambridge, UK, CB3 0FD SOSP'03, Oct. 19-22, 2003, Bolton Landing, New York, USA.

"Design of the EROS Trusted Window System" by Jonathan S. Shapiro, John Vanderburgh, Eric Northrup, Systems Research Laboratory Johns Hopkins University, and, David Chizmadia, Promia, Inc. 2004.

"Survey of System Virtualization" Techniques by Robert Rose Mar. 8, 2004.

White Paper: "Smart Phone Security Issues" by Luc Delpha and Maliha Rasheed, Cyber Risk Consulting Blackhat Briefings Europe May 2004.

"Software Security and Privacy Risks in Mobile E-Commerce" by Anup K. Ghosh and Tara M. Swaminatha, Communications of the ACM Feb. 2001 vol. 44, No. 2.

T. Jaeger, A. D. Rubin, and A. Prakash. "Building systems that flexibly control downloaded executable content." In Proceedings of the 1996 USENIX Security Symposium, pp. 131-148, San Jose, Ca., 1996.

David A. Wagner, "Janus: an approach for confinement of untrusted applications." Master's thesis, University of California, Berkeley, 1999. Also available. Technical Report CSD-99-1056, UC Berkeley, Computer Science Division. http://www.cs.berkeley.edu/~daw/papers/janus-masters.ps.

Richard West and Jason Gloudon, "User-Level Sandboxing: a Safe and Efficient Mechanism for Extensibility", Technical Report, 2003-014, Boston University, Jun. 2003.

Shaya Potter, Jason Nieh, Dinesh Subhraveti, "Secure Isolation and Migration of Untrusted Legacy Applications." Columbia University Technical Report CUCS-005-04, Jan. 2004.

M. Schmid, F. Hill, A. Ghosh, "Protecting Data from Malicious Software." Annual Computer Security Applications Conference (ACSAC'02), Las Vegas, NV, Dec. 2002.

Valentin Razmov "Security in Untrusted Code Environments: Missing Pieces of the Puzzle." Dept. of Computer Science and Engineering, University of Washington, Mar. 30, 2002.

Sotiris Ioannidis and Steven M. Bellovin. "Sub-Operating Systems: A New Approach to Application Security." Technical Report MS-CIS-01-06, University of Pennsylvania, Feb. 2000.

"Spyware, Adware, and Peer to Peer Networks; The Hidden Threat to Corporate Security" by Kevin Townsend, Pest Patrol, 2003.

Beyond Viruses: Why Anti-Virus Software is No Longer Enough by David Stang PhD, Pest Patrol, 2002.

"The Web: Threat or Menace?" from "Firewalls and Internet Security: Repelling the Wiley Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, 2003.

Mehta, N. V., et al., "Expanding and Extending the Security Features of JAVA," Proceedings of the 7th USENIX Security Symposium, San Antonio, Texas Jan. 26-29, 1998, 15 pages.

Kevin Townsend; "Spyware, Adware, and Peer to Peer Networks; The Hidden Threat to Corporate Security" © Pest Patrol, 2003.

David Stang, PhD; "Beyond Viruses: Why Anti-Virus Software is No Longer Enough", © Pest Patrol 2002.

"The Web: Threat or Menace?" From "Firewalls and Internet Security: Repelling the Wiley Hacker", Second Edition, Addison-Wesley, ISBN 0-201-63466-X, 2003 ©.

* cited by examiner

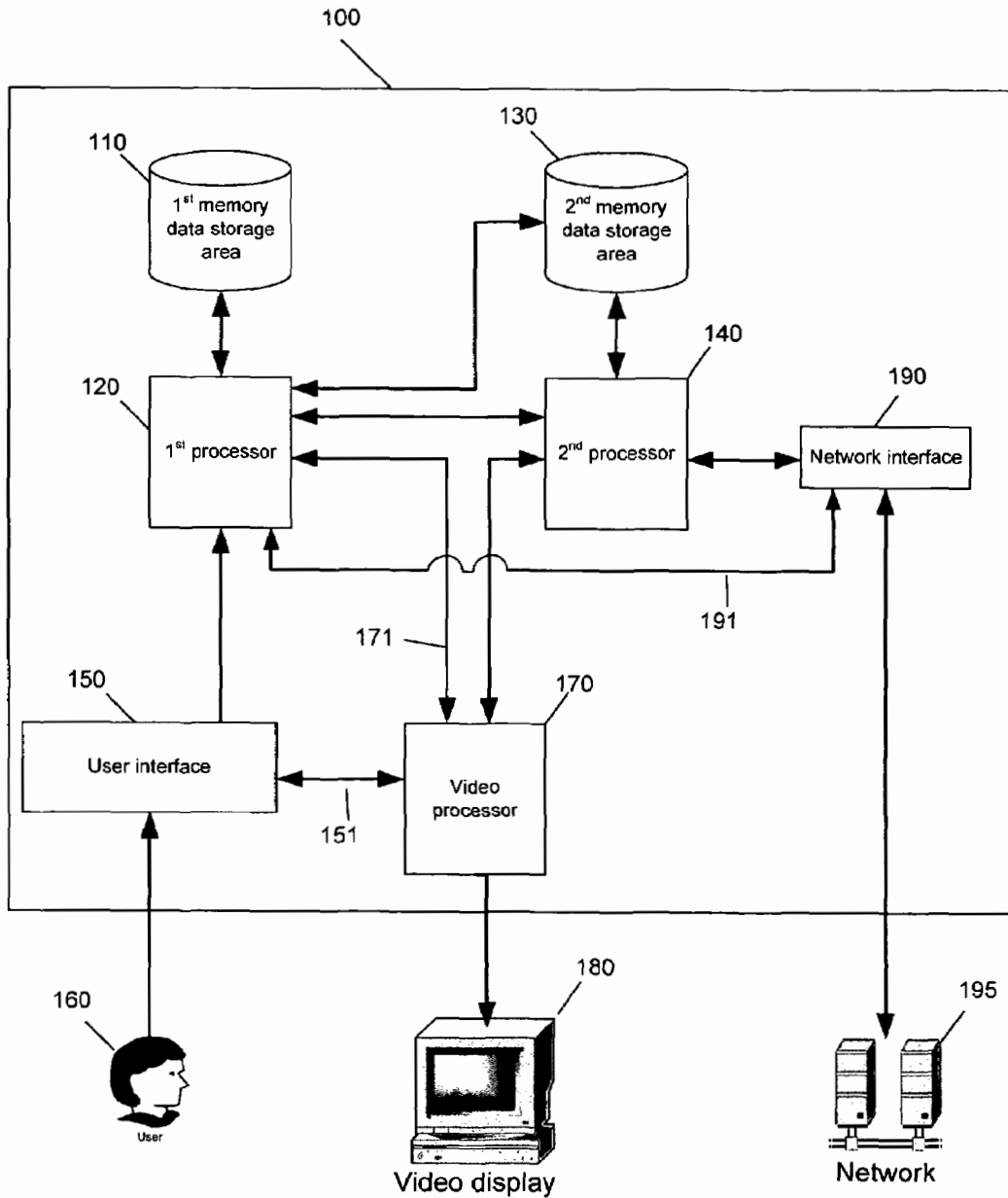100

130

110

1st memory data storage area

2nd memory data storage area

140

120

190

1st processor

2nd processor

Network interface

191

171

150

170

User interface

Video processor

151

160

180

195

User

Video display

Network

Fig. 1

200

210

User opens protected process

220

1st processor (P1) instructs 2nd processor (P2) to initiate protected process and open process window

230

P1 passes user interface data to P2 when P2 window is selected or active

240

P2 generates video data for P2 process window(s) and passes video data to video processor

250

Video processor interleaves video data from all P1 and P2 processes
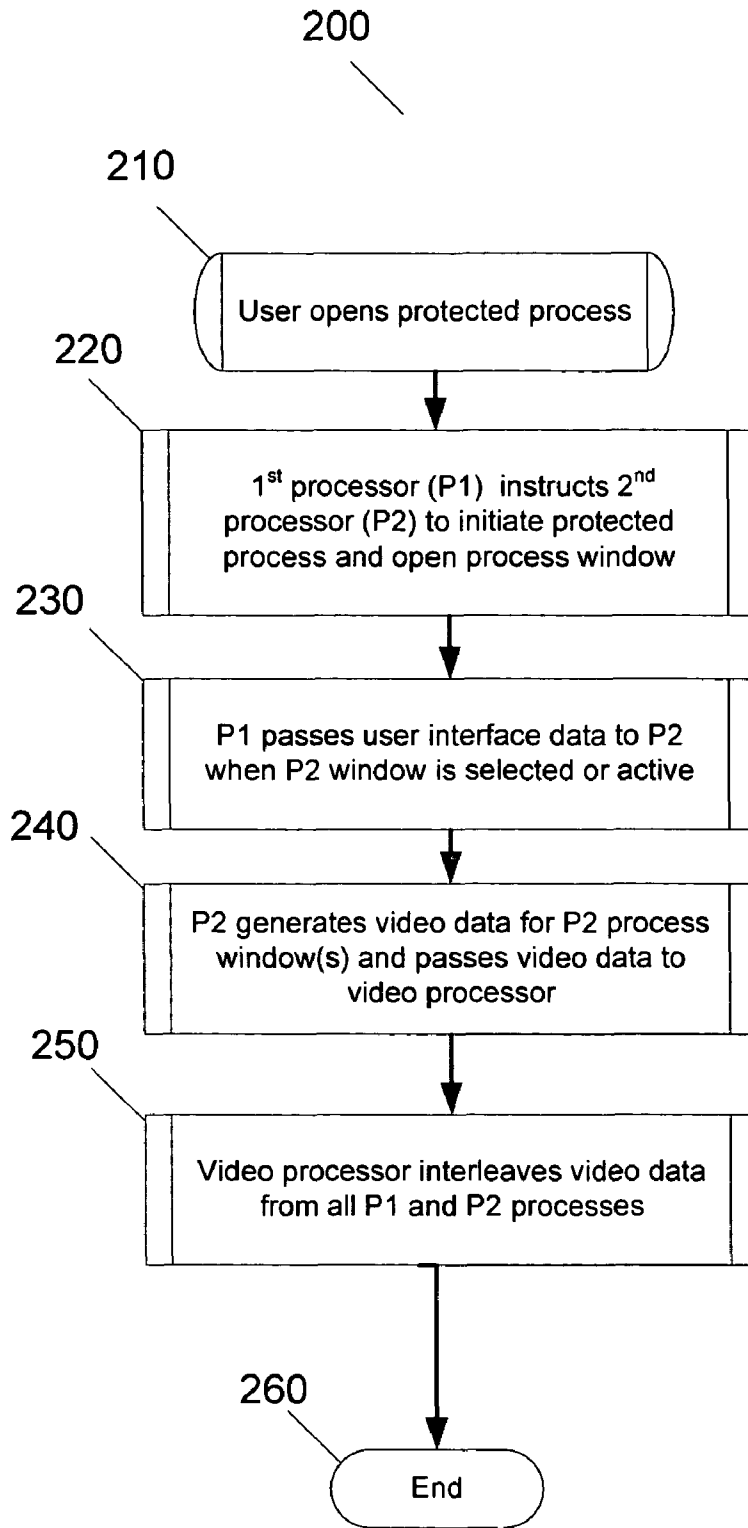
260

End

Fig. 2

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.

fastcase®
Smarter legal research.