



US010318332B2

(12) **United States Patent**  
**Mola**

(10) **Patent No.:** **US 10,318,332 B2**  
(45) **Date of Patent:** **Jun. 11, 2019**

(54) **VIRTUAL MACHINE EXECUTION TRACING**

(71) Applicant: **Microsoft Technology Licensing, LLC**,  
Redmond, WA (US)

(72) Inventor: **Jordi Mola**, Bellevue, WA (US)

(73) Assignee: **Microsoft Technology Licensing, LLC**,  
Redmond, WA (US)

(\*) Notice: Subject to any disclaimer, the term of this  
patent is extended or adjusted under 35  
U.S.C. 154(b) by 86 days.

(21) Appl. No.: **15/488,282**

(22) Filed: **Apr. 14, 2017**

(65) **Prior Publication Data**

US 2018/0285136 A1 Oct. 4, 2018

**Related U.S. Application Data**

(60) Provisional application No. 62/480,408, filed on Apr.  
1, 2017.

(51) **Int. Cl.**  
**G06F 11/36** (2006.01)  
**G06F 9/455** (2018.01)

(52) **U.S. Cl.**  
CPC ..... **G06F 9/45558** (2013.01); **G06F 11/3636**  
(2013.01); **G06F 2009/45591** (2013.01)

(58) **Field of Classification Search**  
CPC ..... **G06F 9/45558**  
See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

4,598,364 A 7/1986 Gum et al.  
5,381,533 A 1/1995 Peleg et al.

5,905,855 A 5/1999 Klaiber et al.  
5,944,841 A 8/1999 Christie  
6,009,270 A 12/1999 Mann  
6,094,729 A 7/2000 Mann

(Continued)

**OTHER PUBLICATIONS**

Xu, et al., "ReTrace: Collecting Execution Trace with Virtual  
Machine Deterministic Replay", In Proceedings of 3rd Annual  
Workshop on Modeling, Benchmarking and Simulation, Jun. 10,  
2007, 8 pages.

(Continued)

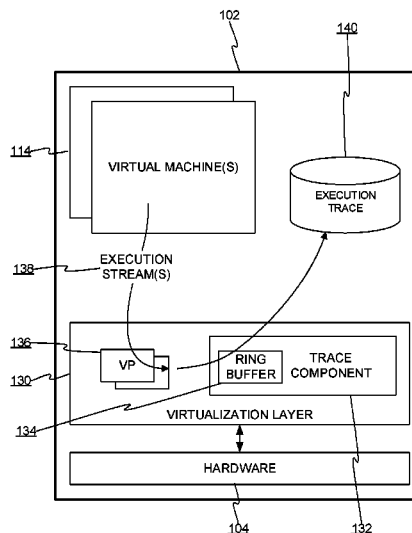
*Primary Examiner* — Sisley N Kim

(74) *Attorney, Agent, or Firm* — Workman Nydegger

(57) **ABSTRACT**

Embodiments relate to a virtualization layer capturing  
replayable execution traces of VMs managed by the virtu-  
alization layer. Execution tracing can be performed on any  
unit of execution managed by the virtualization layer, e.g.,  
threads, processes, virtual processors, individual VMs, mul-  
tiple VMs, etc. Traced execution units may be executing in  
parallel. Execution tracing involves capturing to a buffer:  
executed instructions, memory inputted to instructions,  
memory outputted by instructions, registers touched by  
instructions, and ordering markers. Trace data can be cap-  
tured in chunks, where causality is preserved and ordering is  
preserved between chunks but not necessarily within  
chunks. The chunks may be delineated by inserting mono-  
tonically increasing markers between context switches, thus  
relatively ordering the chunks. Determinism may be par-  
tially provided by identifying non-deterministic events. VM  
tracing may be transparent to guest software, which need not  
be instrumented. Alternatively, guests may interface with the  
virtualization layer to control tracing functionality.

**20 Claims, 5 Drawing Sheets**



(56)

## References Cited

## U.S. PATENT DOCUMENTS

- |                  |         |                           |                  |         |                             |
|------------------|---------|---------------------------|------------------|---------|-----------------------------|
| 6,101,524 A      | 8/2000  | Choi et al.               | 2008/0215920 A1  | 9/2008  | Mayer et al.                |
| 6,167,536 A      | 12/2000 | Mann                      | 2008/0250207 A1  | 10/2008 | Davis et al.                |
| 6,351,844 B1     | 2/2002  | Bala                      | 2008/0256396 A1  | 10/2008 | Giannini et al.             |
| 6,480,886 B1     | 11/2002 | Paice                     | 2008/0270745 A1  | 10/2008 | Saha et al.                 |
| 6,634,011 B1     | 10/2003 | Peltier et al.            | 2008/0288826 A1  | 11/2008 | Nemoto                      |
| 6,728,949 B1     | 4/2004  | Bryant et al.             | 2009/0006729 A1  | 1/2009  | Piazza et al.               |
| 6,772,324 B2     | 8/2004  | Akkary et al.             | 2009/0013133 A1  | 1/2009  | Cypher et al.               |
| 6,854,108 B1     | 2/2005  | Choi                      | 2009/0031173 A1  | 1/2009  | Al-omari et al.             |
| 7,055,070 B1     | 5/2006  | Uhler et al.              | 2009/0037886 A1  | 2/2009  | Mccoy et al.                |
| 7,089,400 B1     | 8/2006  | Pickett et al.            | 2009/0106278 A1* | 4/2009  | Ramacher ..... G06F 11/0748 |
| 7,178,133 B1     | 2/2007  | Thekkath                  | 2009/0138859 A1  | 5/2009  | Chen et al.                 |
| 7,181,728 B1     | 2/2007  | Thekkath                  | 2009/0144742 A1  | 6/2009  | Subhraveti et al.           |
| 7,380,253 B2     | 5/2008  | Yamauchi et al.           | 2009/0319753 A1  | 12/2009 | Welc et al.                 |
| 7,448,025 B2     | 11/2008 | Kalafatis et al.          | 2010/0106912 A1  | 4/2010  | Cypher et al.               |
| 7,454,486 B2     | 11/2008 | Kaler et al.              | 2010/0162247 A1  | 6/2010  | Welc et al.                 |
| 7,478,394 B1     | 1/2009  | de Dinechin et al.        | 2010/0205484 A1  | 8/2010  | Dragicevic et al.           |
| 7,620,938 B2     | 11/2009 | Edwards et al.            | 2010/0223446 A1  | 9/2010  | Katariya et al.             |
| 7,676,632 B2     | 3/2010  | Miller                    | 2010/0250856 A1  | 9/2010  | Owen et al.                 |
| 7,877,630 B1     | 1/2011  | Favor et al.              | 2010/0251031 A1* | 9/2010  | Nieh ..... G06F 11/3419     |
| 7,958,497 B1     | 6/2011  | Lindo et al.              | 2010/0268995 A1  | 10/2010 | Goodman et al.              |
| 7,984,129 B2     | 7/2011  | Vaught                    | 2011/0029821 A1* | 2/2011  | Chow ..... G06F 11/3476     |
| 8,010,337 B2     | 8/2011  | Narayanan et al.          | 2011/0271070 A1  | 11/2011 | Worthington et al.          |
| 8,087,017 B1     | 12/2011 | Whaley et al.             | 2011/0276761 A1  | 11/2011 | Saha et al.                 |
| 8,296,775 B2     | 10/2012 | Thornton et al.           | 2011/0288847 A1  | 11/2011 | Narayanan et al.            |
| 8,423,965 B2     | 4/2013  | Goel et al.               | 2012/0095728 A1  | 4/2012  | Ubukata                     |
| 8,468,501 B2     | 6/2013  | Subhraveti                | 2013/0036403 A1  | 2/2013  | Geist                       |
| 8,484,516 B2     | 7/2013  | Giannini et al.           | 2013/0086567 A1  | 4/2013  | Inoue et al.                |
| 8,499,200 B2     | 7/2013  | Cathro                    | 2014/0040557 A1  | 2/2014  | Frey et al.                 |
| 8,543,988 B2     | 9/2013  | Shimazaki et al.          | 2014/0059523 A1  | 2/2014  | Frazier et al.              |
| 8,612,650 B1     | 12/2013 | Carrie et al.             | 2014/0215443 A1  | 7/2014  | Voccio et al.               |
| 8,719,796 B2     | 5/2014  | Rosu et al.               | 2014/0281710 A1  | 9/2014  | Cain et al.                 |
| 8,769,511 B2     | 7/2014  | Gal et al.                | 2014/0372987 A1  | 12/2014 | Strong et al.               |
| 8,832,682 B2     | 9/2014  | Xu et al.                 | 2015/0012699 A1  | 1/2015  | Rizzo et al.                |
| 9,015,441 B2     | 4/2015  | Worthington et al.        | 2015/0089155 A1  | 3/2015  | Busaba et al.               |
| 9,058,415 B1     | 6/2015  | Serebrin et al.           | 2015/0089301 A1  | 3/2015  | Laurenti                    |
| 9,164,809 B2     | 10/2015 | Tsirkin et al.            | 2015/0319221 A1  | 11/2015 | Zmievski et al.             |
| 9,268,666 B2     | 2/2016  | Law et al.                | 2015/0355996 A1  | 12/2015 | Smith et al.                |
| 9,280,379 B2     | 3/2016  | Tsirkin et al.            | 2015/0378870 A1  | 12/2015 | Marron et al.               |
| 9,300,320 B2     | 3/2016  | Ansari et al.             | 2016/0283748 A1  | 9/2016  | Oh et al.                   |
| 9,329,884 B2     | 5/2016  | Strong et al.             | 2016/0292061 A1  | 10/2016 | Marron et al.               |
| 9,361,228 B2     | 6/2016  | Turner et al.             | 2017/0052876 A1  | 2/2017  | Svensson et al.             |
| 9,535,815 B2     | 1/2017  | Smith et al.              | 2017/0140082 A1  | 5/2017  | Suresh et al.               |
| 9,569,338 B1     | 2/2017  | Bradbury et al.           | 2017/0161173 A1  | 6/2017  | Bradbury et al.             |
| 9,767,237 B2     | 9/2017  | Suresh et al.             | 2017/0192886 A1  | 7/2017  | Boehm et al.                |
| 9,934,127 B1     | 4/2018  | Mola et al.               | 2017/0286111 A1  | 10/2017 | Pereira et al.              |
| 10,031,833 B2    | 7/2018  | Mola et al.               | 2018/0060213 A1  | 3/2018  | Mola                        |
| 10,031,834 B2    | 7/2018  | Mola et al.               | 2018/0060214 A1  | 3/2018  | Mola                        |
| 10,042,737 B2    | 8/2018  | Mola et al.               | 2018/0060215 A1  | 3/2018  | Mola                        |
| 2002/0078124 A1  | 6/2002  | Baylor et al.             | 2018/0113788 A1  | 4/2018  | Mola                        |
| 2002/0124237 A1  | 9/2002  | Sprunt et al.             | 2018/0113789 A1  | 4/2018  | Mola                        |
| 2002/0144101 A1  | 10/2002 | Wang et al.               | 2018/0113806 A1  | 4/2018  | Mola                        |
| 2003/0079205 A1  | 4/2003  | Miyao et al.              | 2018/0113809 A1  | 4/2018  | Mola                        |
| 2003/0126508 A1  | 7/2003  | Litt                      | 2018/0136869 A1  | 5/2018  | Mola                        |
| 2003/0233636 A1* | 12/2003 | Crawford ..... G06F 11/28 | 2018/0314623 A1  | 11/2018 | Mola                        |
|                  |         | 717/130                   | 2019/0004930 A1  | 1/2019  | Mola                        |
|                  |         |                           | 2019/0018755 A1  | 1/2019  | Mola                        |

## OTHER PUBLICATIONS

“Non Final Office Action Issued in U.S. Appl. No. 15/604,408”, dated Jan. 18, 2019, 22 Pages.

“Notice of Allowance Issued in U.S. Appl. No. 15/604,334”, dated Jan. 3, 2019, 9 pages.

Hicks, et al., “Debugging Heterogeneous Applications with Pangaea”, In Proceedings of the Sigmetrics Symposium on Parallel and Distributed Tools, Jan. 1, 1996, pp. 41-50.

“International Search Report and Written Opinion Issued in PCT Application No. PCT/US2018/033997”, dated Dec. 6, 2018, 15 pages.

“7 Recording Inferior’s Execution and Replaying It”, In Tenth Edition Debugging with gdb: the gnu Source-Level Debugger for gdb (GDB) Version 7, Chapter 7, Retrieved Date: May 27, 2016, 6 Pages.

“Elm’s Time Traveling Debugger”, Retrieved from <http://debug.elm-lang.org/>, May 23, 2016, 3 Pages.

(56)

**References Cited****OTHER PUBLICATIONS**

"IntelliTrace", Retrieved from: <https://msdn.microsoft.com/en-us/library/dd264915.aspx>, Nov. 3, 2016, 5 Pages.

"Monitoring redefined", Retrieved From : <https://www.dynatrace.com/blog/tracing-is-the-new-debugging-in-distributed-app-development>, Jun. 14, 2017, 14 Pages.

"lightweight recording & deterministic debugging", Retrieved from <http://rr-project.org/>, May 26, 2016, 4 Pages.

"Non-Final Office Action Issued in U.S. Appl. No. 15/252,998", dated Sep. 20, 2017, 15 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/252,998", dated Apr. 27, 2018, 13 Pages.

"Non-final Office Action Issued in U.S. Appl. No. 15/253,027", dated Oct. 10, 2017, 25 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/253,027", dated Mar. 21, 2018, 12 Pages.

"Non Final Office Action Issued in U.S. Appl. No. 15/298,439", dated Aug. 13, 2018, 8 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/298,439", dated Nov. 6, 2018, 8 Pages.

"Non-final Office Action Issued in U.S. Appl. No. 15/349,555", dated Oct. 6, 2017, 22 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/349,555", dated Mar. 29, 2018, 19 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/433,918", dated Sep. 12, 2018, 9 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/637,376", dated Sep. 12, 2018, 9 Pages.

"Notice of Allowance Issued in U.S. Appl. No. 15/637,376", dated Jun. 14, 2018, 16 Pages.

Barr, et al., "TARDIS: Affordable Time-Travel Debugging in Managed Runtimes", In Proceedings of the 2014 ACM International Conference on Object Oriented Programming Systems Languages & Applications, Oct. 15, 2014, 16 Pages.

Basu, et al., "Karma: Scalable Deterministic Record-Replay", Retrieved From : <http://delivery.acm.org/10.1145/2000000/1995950/p359-basu.pdf>, Jun. 1, 2018, pp. g 359-368.

Brady, Fiorenza, "Cambridge University Study States Software Bugs Cost Economy 312 Billion Per Year", Retrieved from <http://www.prweb.com/releases/2013/1/prweb10298185.htm>, Jan. 8, 2013, 4 Pages.

Charles, "Arun Kishan: Inside Windows 7—Farewell to the Windows Kernel Dispatcher Lock", Retrieved from <https://channel9.msdn.com/shows/Going+Deep/Arun-Kishan-arewell-to-the-Windows-kernel-Dispatcher-Lock/>, Aug. 6, 2009, 9 Pages.

Dimitrov, et al., "Time-Ordered Event Traces: A New Debugging Primitive for Concurrency Bugs", In Proceedings of IEEE International Parallel & Distributed Processing Symposium (IPDPS), May 16, 2011, 11 Pages.

Grabner, Andreas, "Tracing is the new Debugging in Distributed App Development", Retrieved From : <https://www.dynatrace.com/blog/tracing-is-the-new-debugging-in-distributed-app-development>, Dec. 13, 2016, 14 Pages.

Guo, et al., "R2: An Application-Level Kernel for Record and Replay", In Proceedings of the 8th USENIX conference on Operating systems design and implementation, Dec. 8, 2008, 16 Pages.

Hower, et al., "Two hardware-based approaches for deterministic multiprocessor replay", In Proceedings of the Communications of the ACM, vol. 52, Issue 6, Jun. 1, 2009, pp. 93-100.

Jiang, et al., "CARE: Cache Guided Deterministic Replay for Concurrent Java Programs", In Proceedings of the 36th International Conference on Software Engineering, May 31, 2014, 11 Pages.

K., Nance, et al., "Virtual Machine Introspection: Observation or Interference?", In proceedings of IEEE Security & Privacy vol. 6, Issue: 5, Sep. 1, 2008, 2 Pages.

Kleen, Andi, "Adding Processor Trace support to Linux", Retrieved from <https://lwn.net/Articles/648154/>, Jul. 1, 2015, 7 Pages.

Lai, et al., "A Versatile Data Cache for Trace Buffer Support", In Journal of IEEE Transactions on Circuits and Systems, vol. 61, Issue 11, Nov. 2014, pp. 3145-3154.

Lee, et al., "Offline Symbolic Analysis for Multi-Processor Execution Replay", In Proceedings of the 42nd Annual IEEE/ ACM International Symposium on Microarchitecture, Dec. 12, 2009, pp. 564-575.

Liang, et al., "Improved Procedure Placement for Set Associative Caches", In Proceedings of the 47th Design Automation Conference, Jun. 13, 2010., 10 Pages.

Liang, et al., "Instruction Cache Locking Using Temporal Reuse Profile", In Proceedings of the 47th Design Automation Conference, Jun. 13, 2010., pp. 344-349.

Mercer, et al., "Model Checking Machine Code with the GNU Debugger", In Proceedings of the 12th international conference on Model Checking Software, Aug. 22, 2005, 15 Pages.

Narayanasamy, et al., "BugNet: Continuously Recording Program Execution for Deterministic Replay Debugging", In Proceedings of the 32nd annual international symposium on Computer Architecture, Jun. 4, 2005, 12 Pages.

Pavel, Dovgalyuk, "Deterministic Replay of System's Execution with Multi-target QEMU Simulator for Dynamic Analysis and Reverse Debugging, 2012", Retrieved From : <https://pdfs.semanticscholar.org/259f/f151c4f79cdc5ec593bec29650c9643c6043.pdf>, Mar. 30, 2012, 4 Pages.

"International Search Report & Written Opinion for PCT Patent Application No. PCT/US18/024233", dated Sep. 4, 2018, 16 Pages.

"International Search Report and Written Opinion Issued in PCT Application No. PCT/US2017/048094", dated Nov. 10, 2017, 12 Pages.

"International Search Report & Written Opinion Issued in PCT Application No. PCT/US2017/060075", dated Feb. 28, 2018, 11 Pages.

Rivers, et al., "Utilizing Reuse Information in Data Cache Management", In Proceedings of the 12th international conference on Supercomputing, Jul. 13, 1998, pp. 449-456.

Sahuquillo, et al., "The Filter Cache: A Run-Time Cache Management Approach", In Proceedings of 25th Euromicro Conference, Sep. 8, 1999, 8 Pages.

Shaaban, et al., "Improving Trace Cache Hit Rates using the Sliding Window Fill Mechanism and Fill Select Table", In Proceedings of the workshop on Memory system performance, Jun. 8, 2004, pp. 36-41.

Sharma, Suchakrapani Dati., "Hardware Tracing with Intel Processor Trace", Retrieved from [https://hsdm.dorsal.polymtl.ca/system/files/10Dec2015\\_0.pdf](https://hsdm.dorsal.polymtl.ca/system/files/10Dec2015_0.pdf), Dec. 10, 2015, 30 Pages.

Tchagou, et al., "Reducing Trace Size in Multimedia Applications Endurance Tests", In Proceedings of Design, Automation & Test in Europe Conference & Exhibition (DATE), Mar. 9, 2015, 2 Pages.

Uzelac, et al., "Hardware-Based Load Value Trace Filtering for On-the-Fly Debugging", In Proceedings of ACM Transactions on Embedded Computing Systems, vol. 12, Issue 2, May 2013, 18 pages.

\* cited by examiner

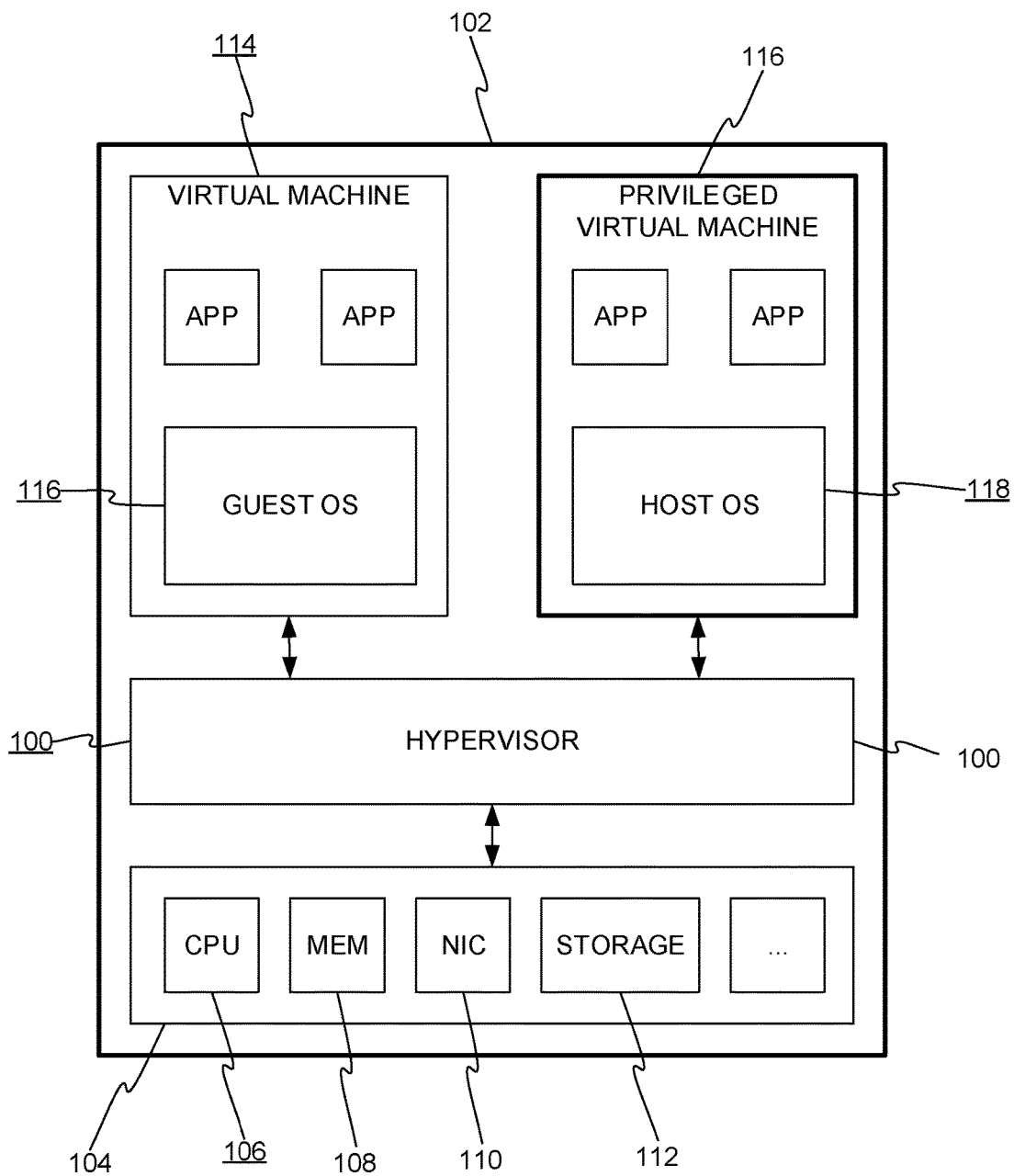


FIG. 1

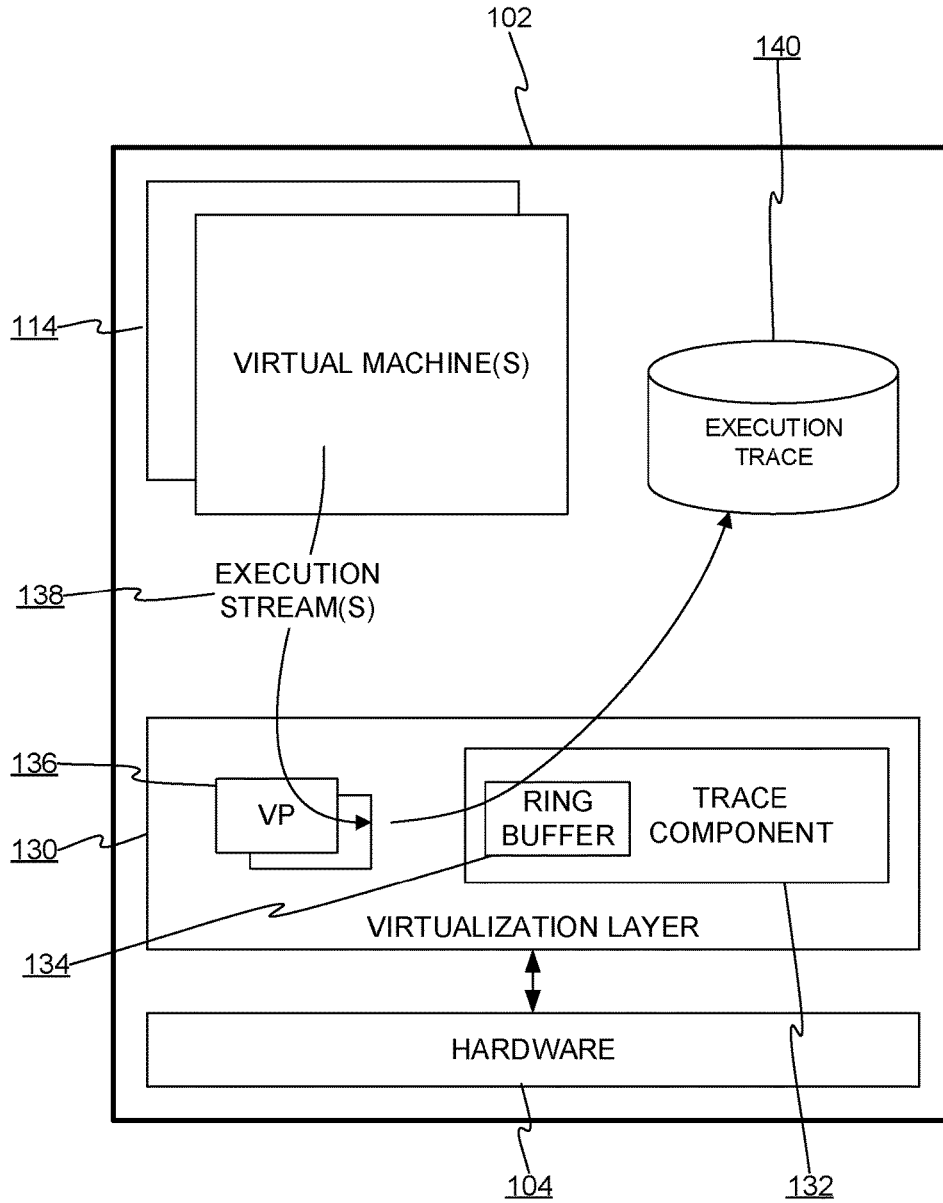


FIG. 2

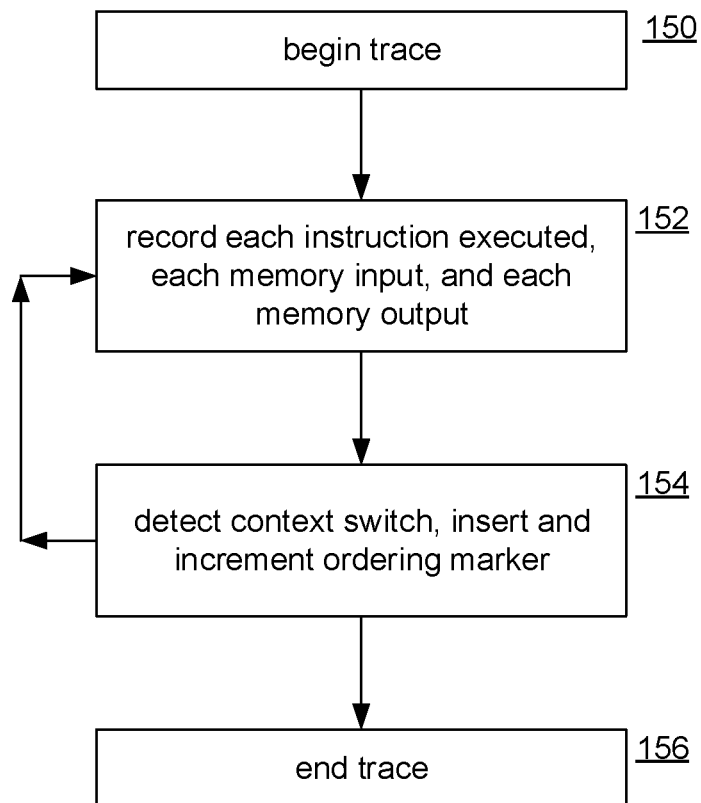


FIG. 3

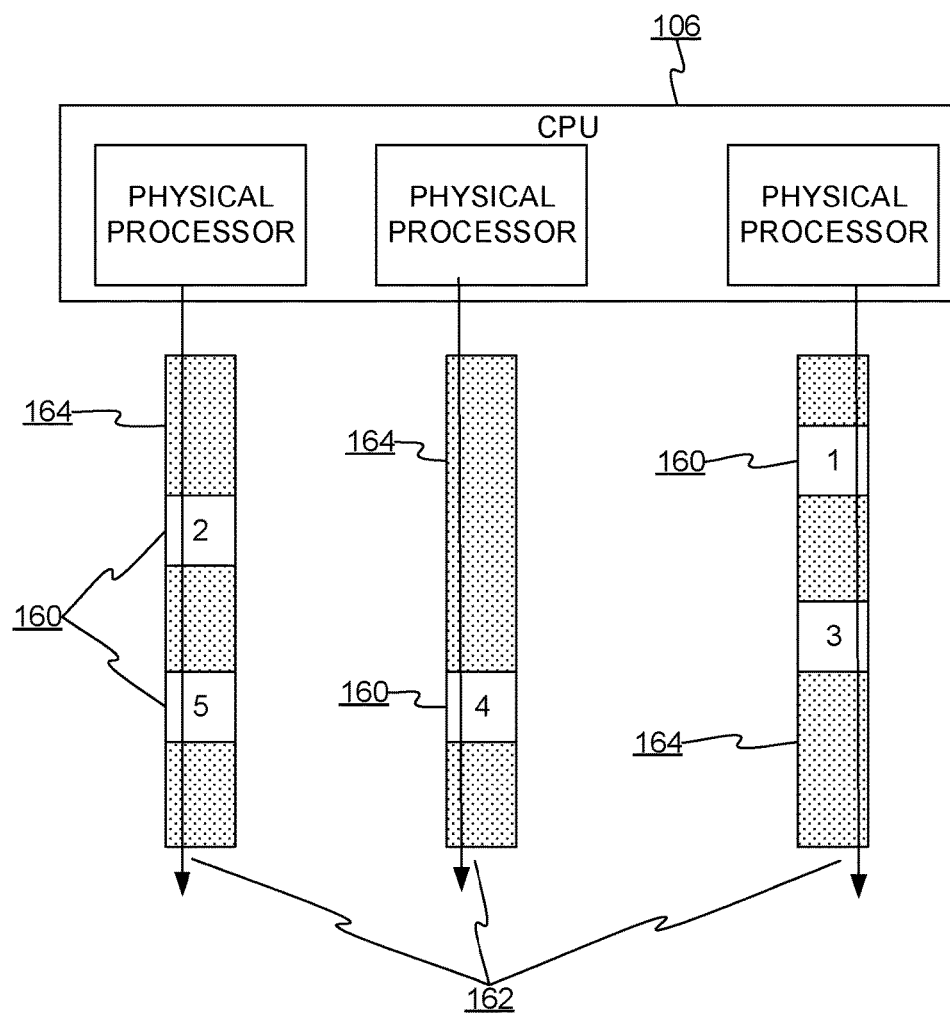


FIG. 4

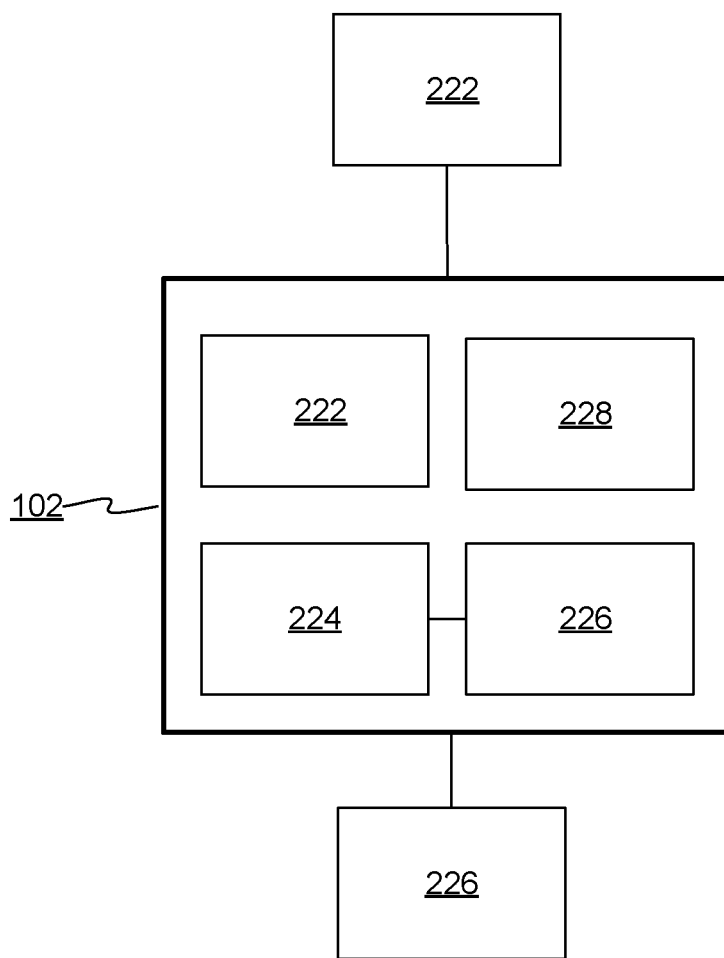


FIG. 5



## VIRTUAL MACHINE EXECUTION TRACING

## RELATED APPLICATION

This application claims an invention which was disclosed in Provisional Application No. 62/480,408, filed Apr. 1, 2017, entitled "VIRTUAL MACHINE EXECUTION TRACING". The benefit under 35 USC § 119(e) of the United States provisional application is hereby claimed, and the aforementioned application is hereby incorporated herein by reference.

## BACKGROUND

Machine virtualization is a technology for presenting the hardware of a computer as multiple virtual machines (VMs) each able to concurrently execute on the same computer. Each such virtual machine (VM) is able to host a guest operating system and the virtualized presentation of the computer's hardware to a guest operating system is mostly transparent to the guest operating system. Machine virtualization has become efficient, reliable, and convenient to manage. Consequently, machine virtualization is being used more often and for expanding types of applications and workloads.

The growing use of machine virtualization has led to increased demand for understanding the execution of a VM, analyzing performance, maintaining a record of a VM's computing activity, and debugging execution of a VM and/or its guest software. VM execution tracing is one technique that has suggested for these purposes. Execution tracing involves tracing the execution activities of a VM and storing the execution trace for later analysis. An execution trace can be used for detailed post-execution analysis and debugging of VM execution. Ideally, an execution trace is deterministic and "replayable", i.e. it has sufficient information to enable playback features commonly found in software debugging tools such as stepwise execution of statements, reverse playback, detailed stack and symbol analysis before and after each statement, etc.

Although VM execution tracing has been recognized as desirable, previous attempts have had shortcomings in implementation and performance. One approach has been to force a VM to execute in a single thread of execution, which facilitates determinism but is difficult to implement and limits performance. For many types of guest software for which parallelism is critical, this limitation prohibits production use. Another approach has been to capture all of a VMs memory, but this carries startup and storage costs. Yet another approach has been to use complex run-time monitoring of memory states to maintain trace determinism, but this is difficult to implement correctly, has high overhead, and can significantly impact the performance of some workloads. Instrument guest software with trace-enabling instructions is another possibility but this has the practical drawback of requiring recompiling and deploying new executable code. Others have tried to interpose trace logic between a VM and a hypervisor, but with mixed success and many platform specificities.

What is needed are techniques for replayable VM execution tracing that are convenient to implement at the virtualization layer, have a low impact on VM performance, maintain causality for concurrent multiprocessing VMs, and can be used with or without VM visibility or actions.

## SUMMARY

The following summary is included only to introduce some concepts discussed in the Detailed Description below.

This summary is not comprehensive and is not intended to delineate the scope of the claimed subject matter, which is set forth by the claims presented at the end.

Embodiments relate to a virtualization layer capturing replayable execution traces of VMs managed by the virtualization layer. Execution tracing can be performed on any unit of execution managed by the virtualization layer, e.g., threads, processes, virtual processors, individual VMs, multiple VMs, etc. Traced execution units may be executing in parallel. Execution tracing involves capturing to a buffer (optionally circular): executed instructions, memory inputted to instructions, memory outputted by instructions, registers touched by instructions, and ordering markers. Execution trace data can be captured in chunks, where causality is preserved and ordering is preserved between chunks but not necessarily within chunks. The chunks may be delineated by inserting monotonically increasing markers between context switches, thus relatively ordering the chunks. Determinism may be partially provided by identifying non-deterministic events. VM tracing may be transparent to guest software, which need not be instrumented. Alternatively, guests may interface with the trace-implementing virtualization layer to control tracing functionality.

Many of the attendant features will be explained below with reference to the following detailed description considered in connection with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present description will be better understood from the following detailed description read in light of the accompanying drawings, wherein like reference numerals are used to designate like parts in the accompanying description.

FIG. 1 shows an example virtualization environment that includes a known type of hypervisor.

FIG. 2 shows a virtualization layer configured for VM execution tracing.

FIG. 3 shows a process for ordering thread traces at the virtualization layer.

FIG. 4 shows ordering markers inserted into traces of respective threads.

FIG. 5 shows details of the computing device on which embodiments described above may be implemented.

## DETAILED DESCRIPTION

Embodiments discussed below relate to tracing execution of virtual machines (VMs) in ways that are efficient, accurately reflect causality. Execution tracing is provided by a trace component within the virtualization layer. The trace component is able to trace parallel VM execution in a way that produces replayable execution traces. A VM may be traced with or without involvement of the guest software within executing within the VM. A trace may be flexibly scoped in terms of when tracing occurs and which VMs or guest software are effectively traced. Several techniques may be used to secure guest data.

FIG. 1 shows an example virtualization environment that includes a known type of hypervisor 100. A computer 102 has hardware 104, including a central processing unit (CPU) 106, memory 108, a network interface 110, non-volatile storage 112, and other components not shown, such as a bus, a display and/or display adapter, etc. The hypervisor 100 manages and facilitates execution of virtual machines (VMs) 114, 116. Each virtual machine 114, 116 typically has virtualized devices including a virtual disk within which a guest/host operating system 116, 118 is stored. Machine or

system virtualization is provided by the hypervisor **100** cooperating with a host operating system **118** that executes in a privileged VM **116**.

The tasks of virtualization may be distributed among the hypervisor **100** and the host operating system **118** in a number of ways. In some cases, the host operating system **118** might consist only of minimal virtualization elements such as tools and user interfaces for managing the hypervisor **100**. In other cases, the host operating system **118** might include one or more of: device virtualization management, inter-VM communication facilities, running device drivers, starting or stopping other VMs, tools for interactive VM management, and others. In short, the guest operating system **118** can potentially handle any virtualization tasks outside core functions of a hypervisor such as CPU and memory sharing. As used herein, “virtualization layer” will refer to any combination of hypervisor and guest VM that collectively provide machine virtualization. The term also refers to virtualization systems that do not use a privileged VM to provide virtualization functionality.

FIG. 2 shows a virtualization layer **130** configured for VM execution tracing. The virtualization layer **130** includes a trace component **132** and ring buffer **134**. Generally, the trace component **132** operates as follows. When a virtual processor **136** of the virtual machine **114** is scheduled for processing time by backing physical processors of the CPU **106**, a context switch occurs for the corresponding guest execution unit (e.g., a thread) and processor instructions of that execution (execution stream **138**) are processed by the backing physical processor (the term “physical processor” as used herein refers to both physical cores and logical cores in the case of hyperthreaded CPUs). The instructions of the execution stream **138** issued by software in the virtual machine are captured by the trace component **132** as they are received or executed and stored in the ring buffer **134**. In one embodiment, instructions are captured using hardware-based trace features of the CPU. In another embodiment, the virtualization layer implements processor emulation and the instruction capturing is built into the processor emulator. In most cases, all instructions are captured when execution tracing is in effect. Execution trace data in the ring buffer **134** may be selective or continuously stored as a persistent execution trace **140** in some local (e.g., a privileged VM’s filesystem) or network storage.

Although a ring buffer is convenient and provides certain advantages, other types of buffers may be used. Full tracing likely will not require a circular buffer. As discussed below, buffering can be useful for selective tracing where a particular scope of execution is to be traced (e.g., certain modules, processes, threads, VMs, etc.).

In addition to capturing instructions the execution trace will include data in memory that is touched by the execution of the thread or other execution unit. This involves, instead of copying all memory of the VM **114**, copying each piece of memory as it is accessed by the execution being traced; conceptually, the inputs and outputs of the instructions are captured as they are being consumed. (perhaps with compression). Accessed register contents are also captured. Each thread generally consumes its own memory in its own way, and what the other threads do is irrelevant. If a kernel call or another thread modifies the traced thread’s memory then those external memory modifications can be captured by the trace component **132**. For additional details see U.S. patent application Ser. No. 15/252,998, titled, “PROGRAM TRACING FOR TIME TRAVEL DEBUGGING AND ANALYSIS” (filed Aug. 31, 2016), and Ser. No. 15/253,027, titled “CACHE-BASED TRACING FOR TIME TRAVEL

DEBUGGING AND ANALYSIS” (filed Aug. 31, 2016), and both incorporated herein by reference.

In one embodiment, all of the execution of a target VM is traced. Because the virtualization layer **130** knows when the CPU is executing instructions from the target VM, the virtualization layer **130** knows when to perform tracing (when the target VM is executing) and when not to. Thus, the generated trace includes only the activities of the target VM. Even if the target VM has multiple virtual processors (VPs) the virtualization layer **132**, which handles CPU scheduling, knows when a VP is executing code for the target VM and traces accordingly. Each thread or execution unit of the target virtual machine is recorded as a separate respective trace set and contains the instructions, memory/registers consumed by same, etc. Post-trace symbol analysis (e.g., during later debugging) can be enabled by recording information that associates each traced instruction with an identifier indicating the executable file or object model or the like that provided the instruction. This allows later reconstruction of symbols from the trace in the same way debuggers provide symbol information.

Most traced execution will have some non-deterministic events that will have to be handled. Non-deterministic instructions are instructions whose output depends on information outside the information that is being tracked for tracing. A first step handling on-deterministic instructions is identifying instructions as such. Once a non-deterministic instruction is detected, the side effects thereof are recorded in the trace and the side effects are reproduced during replay. For example, if an instruction is found to generate a random number, that may be hard to replay with the precision of the original instruction result, so one solution is to record the side effects (in this example, the value of the registry where the random number is located) and at replay time we that number is placed in the appropriate register instead of (or after) executing the original instruction. Another example would be a trace of instruction to read a processor timer. If this is not fully tracked then the side effect can be placed in the trace and at replay time the side effect is used instead of reading the processor timer.

Tracing multiple concurrent threads/VPs presents issues of ordering and causality. If two threads of execution of a traced VM are executing concurrently they can potentially overlap. In order to enable reasoning through causalities in the traces of the respective threads, order of execution is important to consider. While it is possible to include a rich set of trace information to strictly order threads among themselves in a deterministic way, a less burdensome approach is to model trace access to memory in a way that enables sufficient relative ordering for causality without requiring strict ordering relative to all instructions. This can be done by implementing modelling memory for tracing such that reading from memory has acquire semantics and writing to memory has release semantics and ordering and recording those corresponding events. See the aforementioned patent applications for additional details. Because the tracing is done at the virtualization layer the threads/VPs are traced from a common view of causality at the virtualization layer. This same approach can be used not only to order execution of threads of a given VM, but also to order execution of threads of concurrent VMs relative to each other.

Because tracing occurs at the virtualization layer or hypervisor, threads are threads and can be traced regardless of VM execution since memory can be ordered across any two threads. Thus, causality-preserving tracing across machines is possible. This can enable new types of debug-

ging not previously possible. The interactions between software on two different machines (albeit virtual) can be closely correlated.

FIG. 3 shows a process for ordering thread traces at the virtualization layer. At step 150 tracing begins for whichever VM threads start executing. At step 152 execution tracing is performed as discussed above; thread instructions, memory accesses, registers, etc. are recorded as executed in sets for each respective thread. At step 154 a context switch is detected. Each time a context switch is detected, an ordering marker is inserted into the corresponding thread and an incremented value of the inserted ordering marker is stored and then similarly used the next time an ordering marker is needed. Not that an ordering marker may be inserted into a swapped-in thread, a swapped-out thread, or both. This continues for each thread until it ends at step 156.

FIG. 4 shows ordering markers 160 inserted into traces 162 of respective threads. Each trace segment 164 (shaded portion) represents a segment of traced instructions and corresponding input/output data that occurs in a same processor context. While strict ordering might not be guaranteed among instructions in a trace segment 164, ordering among the trace segments 164 (with respect to each other) is guaranteed by the ordering markers 160. The context switches represented by the ordering markers 160 may be a switch due to a guest switching threads, CPU scheduling (timeslicing) by the virtualization layer, etc. The ordering markers may be numbers in any monotonically increasing sequence. The markers might be a global value that increments once for each context switch. For some CPUs, the markers might be timestamp counters provided by the CPU (consistent across all CPU cores). Although all instructions of a trace of a VM or a thread might not be fully ordered, partial ordering and causality is assured, including among VMs if multiple VMs are being traced. Note that the degree to which causality is assured may depend on the memory model that is selected and the amount of analysis a user is willing to do on the trace.

Using the trace techniques described above, a variety of trace control functions (described below) may be implemented by the virtualization layer and/or by a privileged VM that provides virtualization functionality as discussed above. The trace control functions control when and/or how tracing is performed or stored. The trace control functions may be implemented by combinations of hypervisor hypercalls, virtualization interfaces exposed by a privileged VM, etc. Although, guests may be instrumented to take advantage of any trace control functions, the trace control functions may instead be invoked by a privileged VM to control tracing for un-instrumented guests. The trace functions described next may be invoked by an instrumented guest or for an un-instrumented by the privileged VM. If the virtualization layer and/or privileged VM provide an interface for invoking trace functions, such interfaces might be in the form of a user interface provided by the privileged VM, through a REST API (Representational State Application Programming Interface), a virtual device driver, a network port, or any other mechanism to communicate with the virtualization layer to control tracing.

Before describing the trace functions, the use of the ring buffer 134 will be explained. The ring buffer is a buffer for storing a forward moving window of execution traces. In some embodiments, the ring buffer may be in continuous use but without persisting the trace data stored in the buffer. The buffer stores trace data in case tracing is invoked during execution of a target VM. The ring buffer is also useful for buffering data that might be needed for capturing trace data.

For instance, tracing a non-deterministic event might require access to buffered data that would not otherwise be available at the time of the event. The ring buffer may use keyframes to handle wrapping. For example, a keyframe might be added at every 10% chunk of the buffer so that only 10% of the buffer is lost as each new piece of data is added. The ring buffer is also a useful place for performing compression (see above-referenced patent applications) and/or for performing encryption (discussed below).

One of the trace functions is a simple on/off function for turning tracing on or off. The on/off function may have a variety of parameters. One parameter may be the target to be traced. The target may be one or more identified individual VMs or the calling VM (implicit). The target might be an individual process or set of processes. Another parameter may be time extents of the trace. The time might be defined as a time range, for instance, a duration (including possibly backward in time as permitted by how far back the contents of the ring buffer go).

Another trace function is a periodic trace function. Tracing can be activated for periods of time to sample trace data. For example, tracing might be captured 1 second per minute, 10 minutes once per hour, etc. The ring buffer may be in effect for sufficient encompassing time periods to enable the sampling.

Yet another trace function is event-based tracing. Tracing can be linked to identified events such as hypercalls, interrupts, system events (e.g., a process crash) or the like to automatically trace data at times linked to the identified events. Note that any of the trace functions above can potentially be scoped in the same way as the on/off function. That is, any type of trace control may be scoped to a particular process, VM, particular processes on any VMs, a defined VM set, etc. Event-based tracing and other functions for ad hoc trace recording may require that tracing is being performed in the ring buffer and trace data from the ring buffer is only persisted when needed.

Still another trace function is trace encryption. Because VMs may be in different security domains and cross-VM data leaks would be considered security breaches, it is possible for the virtualization layer to encrypt trace data from memory (i.e., instruction inputs and outputs, as well as registers) before it is stored for later post-processing analysis. If the virtualization layer has a key that is private to a VM, the key can be used to encrypt at least the data of a trace of that VM. A debugger configured with a decryption module can potentially use the key to perform debugging on the encrypted trace data. In one embodiment, encryption is used when a non-instrumented VM is traced at the request of another VM. That is, security measures can be triggered based on the relative security levels of the traced VM and the trace-requesting VM.

It should be noted that the trace techniques described herein do not require that the virtualization layer run directly on hardware. Nested VMs can use the same techniques without modification. In other words, a virtualization layer executing within a VM may itself perform tracing of its VMs. If CPU hardware tracing is to be used, the CPU trace features may be used whenever the nested virtualization layer has a slice of CPU time.

FIG. 5 shows details of the computing device 102 on which embodiments described above may be implemented. The technical disclosures herein will suffice for programmers to write software, and/or configure reconfigurable processing hardware (e.g., field-programmable gate arrays (FPGAs)), and/or design application-specific integrated cir-

cuits (ASICs), etc., to run on the computing device **220** to implement any of the features or embodiments described herein.

The computing device **102** may have one or more displays **222**, a network interface **224** (or several), as well as storage hardware **226** and processing hardware **228**, which may be a combination of any one or more: central processing units, graphics processing units, analog-to-digital converters, bus chips, FPGAs, ASICs, Application-specific Standard Products (ASSPs), or Complex Programmable Logic Devices (CPLDs), etc. The storage hardware **226** may be any combination of magnetic storage, static memory, volatile memory, non-volatile memory, optically or magnetically readable matter, etc. The meaning of the term “storage”, as used herein does not refer to signals or energy per se, but rather refers to physical apparatuses and states of matter. The hardware elements of the computing device **102** may cooperate in ways well understood in the art of machine computing. In addition, input devices may be integrated with or in communication with the computing device **102**. The computing device **102** may have any form-factor or may be used in any type of encompassing device. The computing device **102** may be in the form of a handheld device such as a smartphone, a tablet computer, a gaming device, a server, a rack-mounted or backplaned computer-on-a-board, a system-on-a-chip, or others.

Embodiments and features discussed above can be realized in the form of information stored in volatile or non-volatile computer or device readable storage hardware. This is deemed to include at least hardware such as optical storage (e.g., compact-disk read-only memory (CD-ROM)), magnetic media, flash read-only memory (ROM), or any means of storing digital information in to be readily available for the processing hardware **228**. The stored information can be in the form of machine executable instructions (e.g., compiled executable binary code), source code, byte-code, or any other information that can be used to enable or configure computing devices to perform the various embodiments discussed above. This is also considered to include at least volatile memory such as random-access memory (RAM) and/or virtual memory storing information such as central processing unit (CPU) instructions during execution of a program carrying out an embodiment, as well as non-volatile media storing information that allows a program or executable to be loaded and executed. The embodiments and features can be performed on any type of computing device, including portable devices, workstations, servers, mobile wireless devices, and so on.

The invention claimed is:

**1.** A method performed by a computing device comprising processing hardware and storage hardware, the method comprising:

executing a virtualization layer that manages execution of a plurality of virtual machines on the processing hardware, the plurality of virtual machines comprising a first virtual machine comprising a respective first virtual processor and a respective first guest operating system and a second virtual machine comprising a respective second virtual processor and a respective second guest operating system;

switching, by the virtualization layer, to a first execution context of the first virtual machine, to enable the first guest operating system to issue a plurality of first instructions to the first virtual processor;

based on the plurality of first instructions being executed by the first virtual processor, recording first execution trace data comprising (i) the plurality of first instructions

executed by the first virtual processor, (ii) first memory portions selected for tracing on the basis of the first memory portions storing inputs and/or outputs of the plurality of first instructions, and (iii) a plurality of first ordering markers inserted into the first execution trace data by the virtualization layer, each of the plurality of first ordering markers corresponding to a respective determination that a first orderable event has occurred between two or more of the plurality of first instructions;

switching, by the virtualization layer, to a second execution context of the second virtual machine, to enable the second guest operating system to issue a plurality of second instructions to the second virtual processor; and based on the plurality of second instructions being executed by the second virtual processor, recording second execution trace data comprising (i) the plurality of second instructions executed by the second virtual processor, (ii) second memory portions selected for tracing on the basis of the second memory portions storing inputs and/or outputs of the plurality of second instructions, and (iii) a plurality of second ordering markers inserted into the second execution trace data by the virtualization layer, each of the plurality of second ordering markers corresponding to a respective determination that a second orderable event has occurred between two or more of the plurality of second instructions,

wherein the plurality of first ordering markers and the plurality of second ordering markers also enable a determination of causality between the first orderable event at the first virtual machine and the second orderable event at the second virtual machine.

**2.** A method according to claim **1**, wherein at least one of the first or second orderable events comprises a context switch.

**3.** A method according to claim **2**, wherein the context switch comprises a thread context switch.

**4.** A method according to claim **1**, wherein at least one of the first or second orderable event comprises an element of a memory model implemented by the virtualization layer to record the execution trace data.

**5.** A method according to claim **1**, wherein the virtualization layer comprises an application programming interface (API) comprising a call, the method further comprising invoking the call by the first virtual machine, and based on the first virtual machine invoking of the call, performing the recording of the execution trace data.

**6.** A method according to claim **5**, wherein the invocation of the call turns the recording of the execution trace data on or off, or sets a scope of execution to be traced.

**7.** A method according to claim **1**, further comprising recording the execution trace data to a circular buffer and copying execution trace data from the circular buffer to persistent storage.

**8.** A computer system comprising:

one or more processors; and

one or more computer-readable media having stored thereon computer-executable instructions that are executable by the one or more processors to cause the computer to perform the following:

execute a virtualization layer that manages execution of a plurality of virtual machines on the processing hardware, the plurality of virtual machines comprising a first virtual machine comprising a respective first virtual processor and a respective first guest operating system and a second virtual machine comprising a

respective second virtual processor and a respective second guest operating system;  
 switch, by the virtualization layer, to a first execution context of the first virtual machine, to enable the first guest operating system to issue a plurality of first instructions to the first virtual processor;  
 based on the plurality of first instructions being executed by the first virtual processor, record first execution trace data comprising (i) the plurality of first instructions executed by the first virtual processor, (ii) first memory portions selected for tracing on the basis of the first memory portions storing inputs and/or outputs of the plurality of first instructions, and (iii) a plurality of first ordering markers inserted into the first execution trace data by the virtualization layer, each of the plurality of first ordering markers corresponding to a respective determination that a first orderable event has occurred between two or more of the plurality of first instructions;  
 switch, by the virtualization layer, to a second execution context of the second virtual machine, to enable the second guest operating system to issue a plurality of second instructions to the second virtual processor; and  
 based on the plurality of second instructions being executed by the second virtual processor, record second execution trace data comprising (i) the plurality of second instructions executed by the second virtual processor, (ii) second memory portions selected for tracing on the basis of the second memory portions storing inputs and/or outputs of the plurality of second instructions, and (iii) a plurality of second ordering markers inserted into the second execution trace data by the virtualization layer, each of the plurality of second ordering markers corresponding to a respective determination that a second orderable event has occurred between two or more of the plurality of second instructions,  
 wherein the plurality of first ordering markers and the plurality of second ordering markers also enable a determination of causality between the first orderable event at the first virtual machine and the second orderable event at the second virtual machine.

9. A computer system according to claim 8, wherein at least one of the first or second orderable events comprises a context switch.

10. A computer system according to claim 9, wherein the context switch comprises a thread context switch.

11. A computer system according to claim 8, wherein at least one of the first or second orderable event comprises an element of a memory model implemented by the virtualization layer to record the execution trace data.

12. A computer system according to claim 8, wherein the virtualization layer comprises an application programming interface (API) comprising a call, the computer-executable instructions also being executable by the one or more processors to invoke the call by the first virtual machine, and based on the first virtual machine invoking of the call, perform the recording of the execution trace data.

13. A computer system according to claim 12, wherein the invocation of the call turns the recording of the execution trace data on or off, or sets a scope of execution to be traced.

14. A computer system according to claim 8, the computer-executable instructions also being executable by the one or more processors to record the execution trace data to a circular buffer and copy execution trace data from the circular buffer to persistent storage.

15. A computer program product comprising one or more hardware storage devices having stored thereon computer-executable instructions that are executable by one or more processors to cause a computer to perform the following:

execute a virtualization layer that manages execution of a plurality of virtual machines on the processing hardware, the plurality of virtual machines comprising a first virtual machine comprising a respective first virtual processor and a respective first guest operating system and a second virtual machine comprising a respective second virtual processor and a respective second guest operating system;

switch, by the virtualization layer, to a first execution context of the first virtual machine, to enable the first guest operating system to issue a plurality of first instructions to the first virtual processor;

based on the plurality of first instructions being executed by the first virtual processor, record first execution trace data comprising (i) the plurality of first instructions executed by the first virtual processor, (ii) first memory portions selected for tracing on the basis of the first memory portions storing inputs and/or outputs of the plurality of first instructions, and (iii) a plurality of first ordering markers inserted into the first execution trace data by the virtualization layer, each of the plurality of first ordering markers corresponding to a respective determination that a first orderable event has occurred between two or more of the plurality of first instructions;

switch, by the virtualization layer, to a second execution context of the second virtual machine, to enable the second guest operating system to issue a plurality of second instructions to the second virtual processor; and

based on the plurality of second instructions being executed by the second virtual processor, record second execution trace data comprising (i) the plurality of second instructions executed by the second virtual processor, (ii) second memory portions selected for tracing on the basis of the second memory portions storing inputs and/or outputs of the plurality of second instructions, and (iii) a plurality of second ordering markers inserted into the second execution trace data by the virtualization layer, each of the plurality of second ordering markers corresponding to a respective determination that a second orderable event has occurred between two or more of the plurality of second instructions,

wherein the plurality of first ordering markers and the plurality of second ordering markers also enable a determination of causality between the first orderable event at the first virtual machine and the second orderable event at the second virtual machine.

16. A computer program product according to claim 15, wherein at least one of the first or second orderable events comprises a context switch.

17. A computer program product according to claim 15, wherein at least one of the first or second orderable event comprises an element of a memory model implemented by the virtualization layer to record the execution trace data.

18. A computer program product according to claim 15, wherein the virtualization layer comprises an application programming interface (API) comprising a call, the computer-executable instructions also being executable by the one or more processors to invoke the call by the first virtual machine, and based on the first virtual machine invoking of the call, perform the recording of the execution trace data.

**11****12**

**19.** A computer program product according to claim **18**, wherein the invocation of the call turns the recording of the execution trace data on or off, or sets a scope of execution to be traced.

**20.** A computer program product according to claim **15**,  
the computer-executable instructions also being executable  
by the one or more processors to record the execution trace  
data to a circular buffer and copy execution trace data from  
the circular buffer to persistent storage.

\* \* \* \* \*

10