Device Driver isolation using virtual machines

Sushrut Shirole

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Science & Applications

Dr. Godmar Back, Chair
Dr. Keith Bisset
Dr. Kirk Cameron

Dec 12, 2013
Blacksburg, Virginia

Keywords: Device driver, Virtual machines, domain,

Device driver isolation using virtual machines.

Sushrut Shirole

(ABSTRACT)

In majority of today's operating system architectures, kernel is tightly coupled with the device drivers. In such cases, failure in critical components can lead to system failure. A malicious or faulty device driver can make the system unstable, thereby reducing the robustness. Unlike user processes, a simple restart of the device driver is not possible. In such circumstances a complete system reboot is necessary for complete recovery. In a virtualized environment or infrastructure where multiple operating systems execute over a common hardware platform, cannot afford to reboot the entire hardware due to a malfunctioning of a third party device driver.

The solution we implement exploits the virtualization to isolate the device drivers from the kernel. In this implementation, a device driver serves the user process by running in a separate virtual machine and hence is isolated from kernel. This proposed solution increases the robustness of the system, benefiting all critical systems.

To support the proposed solution, we implemented a prototype based on linux kernel and Xen hypervisor. In this prototype we create an independent device driver domain for Block device driver. Our prototype demonstrate that a block device driver can be run in a separate domain.

We isolate device drivers from the kernel with two different approaches and compare both the results. In first approach, we implement the device driver isolation using an interrupt-based inter-domain signaling facility provided by xen hypervisor called event channels. In second approach, we implement the solution, using spinning threads. In second approach user application puts the request in request queue asynchronously and independent driver domain spins over the request queue to check if a new request is available. Event channel is an interrupt-based inter-domain mechanism and it involves immediate context switch, however, spinning doesn't involve immediate context switch and hence can give different results than event channel mechanism.

Acknowledgments

Acknowledgments goes here

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A system is judged by the quality of the services it offers and its ability to function reliably. Even though reliability of operating systems has been studied for several decades, it remains a major concern today. The characteristics of operating systems which make them unstable are size and complexity.

Software reliability study shows that 6 to 16 number of errors/1000 executable lines can be found within a module[6][32]. Linux kernel has over 15 million lines of code. If we assume minimum estimate, Linux kernel has around 90,000 bugs. Researchers have shown that the error rate for device drivers is higher than the error rate for the rest of the kernel[11]. Considering the fact that the operating system predominantly consists of device drivers, the faults in device drivers make the operating system unreliable[11].

1.1 Problem Statement

In order to make a system reliable, it is essential that a device driver code does not contain any bug. However, finding all these bugs and fixing them is difficult since bug fixes introduces new lines of code resulting in new bugs.
In modern operating systems memory protection is a way to control memory access rights. The memory protection prevents a process from accessing memory that has not been allocated to it. The memory protection prevents a bug within a process from affecting other processes, or the operating system[14][28]. Monolithic kernel component do not have the same level of isolation the user level applications have. Unlike user applications, monolithic kernel has hundreds of procedures linked together. As a result, any portion of the kernel can access and potentially overwrite any kernel data structure used by an unrelated component. Such a non-existent isolation between kernel and device driver causes a bug in device drivers to corrupt the memory of the other kernel components. This memory corruption might lead to system crash. Hence the underlying cause of unreliability in the operating system is the tight coupling between device driver and Linux kernel.

1.2 Proposed Solution

The reliability of a system can be improved by executing device drivers in an isolated environment from the kernel. The dependency of device drivers on other kernel components such as memory management, scheduler etc. make it difficult to isolate device drivers from the kernel.

Our solution here adapts the concept of 'virtualization based fault protection in operating systems' proposed by LeVasseur et. al. [22], Tanenbaum et. al.[32], Nooks[31], Soltesz et. al. [29]. The solution we implement runs a special program called hypervisor. Hypervisor is commonly used to run multiple operating systems in parallel, by exploiting the hardware. The use of virtual machines has a well-deserved reputation for extremely good fault isolation. Since none of the virtual machines are aware of the other virtual machines, malfunctioning of one virtual machine cannot spread to the others.

In a virtualized environment, all virtual machines run as separate user processes in different address spaces. Thus, to exploit the memory protection capability between virtual machines, we run a device driver with minimalistic kernel in one virtual machine, and run user applications and a kernel together in the other virtual machine. As a result, a device driver is isolated from the Linux kernel, making it impossible for the device driver to corrupt any kernel data structure in the virtual machine running user applications.

1.3 Core Contributions

The core contributions of this project can be divided into two parts.

1. The implementation of the device driver isolation concept using two approaches.
2. The performance comparison of the approaches.

The first approach implements device driver isolation using interrupt based communication between front end and back end device drivers. Xen uses the same approach for implementation of the driver domain[1]. This interrupt based model requires context switches[4]. The second approach implements the communication between front end and back end device drivers using spinning of threads. The spinning based model does not require the context switches. This report presents the performance comparison of both the approaches. In addition, the report aims to find if the performance degradation can be attributed to the context switches.

1.4 Organization

This section gives the organization and roadmap of the thesis.

1. Chapter 2 gives the background on memory protection, virtualization, Xen Hypervisor, inter-domain communication, processes and threads.
2. Chapter 3 gives the introduction to design of the system to isolate device driver.
3. Chapter 4 discusses the detailed design and implementation to isolate device driver.
4. Chapter 5 evaluates the performance of Independent device driver with different designs.
5. Chapter 6 reviews the related work in the area of kernel fault tolerance.
6. Chapter 7 concludes the report and lists down the topics where this work can be extended.

Chapter 2

Background

This section gives a background on operating system concepts such as Memory protection, Virtualization, Hypervisor, Processes and threads.

2.1 Memory protection

The memory protection mechanisms of computer systems control the access to objects. The main goal of memory protection is to prevent malicious misuse of the system by users or programs. Memory protection also ensures that each shared resource is used only in accordance with system policies. In addition, it also helps to ensure that errant programs cause minimal damage. However, memory protection systems only provide the mechanisms for enforcing policies and ensuring reliable systems. It is up to administrators, programmers and users to implement those mechanisms[28][18]. The following subsections explain how these policies are implemented at kernel level and user level.

2.1.1 User level

Typically in a monolithic kernel, the lowest X GB of memory is reserved for user processes (In 32-bit architecture 3GB is reserved for user level). The upper $'VM - X'$ GB is reserved for kernel (In 32 bit architecture 1 GB is reserved for kernel). This upper 1 GB is restricted

to $CPL0$ ($ring0$) only. The kernel puts its private data structures in the upper 1GB and always accesses them at the same virtual address, irrespective of what processes are running. At user space, each application runs as a separate process. Each process is associated with an address space and believes that it owns the entire memory, starting with the virtual address 0. However, a translation table translates every memory reference by these processes from virtual to physical addresses. The translation table maintains $< base, bound >$ entry. If a process tries to access virtual address which is out of $'base + bound'$ then error is reported by the OS, otherwise physical address $'base + virtualaddress'$ is returned. This allows multiple processes to be in memory with protection. Since address translation provides protection, a process cannot access to other processes addresses, nor about the OS addresses.
Consider an example in below diagram.

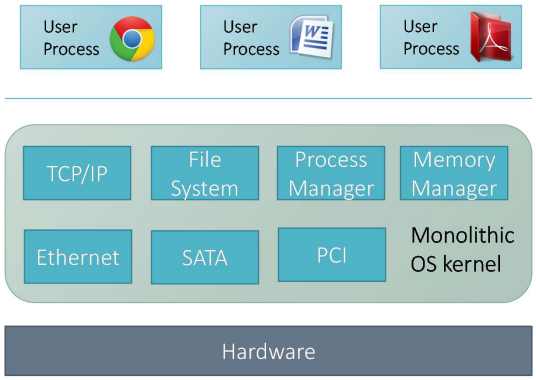

Figure 2.1: User space

In the above system Chromium browser, word processor and pdf reader are running as a 3 different processes in user space.

The word process hits a bug and tries to corrupt the memory out of the address space.

Since the access to the address is restricted because of memory protection, the word processor does not crash the other application or system.

The bug in the word processor might lead to crashing itself.

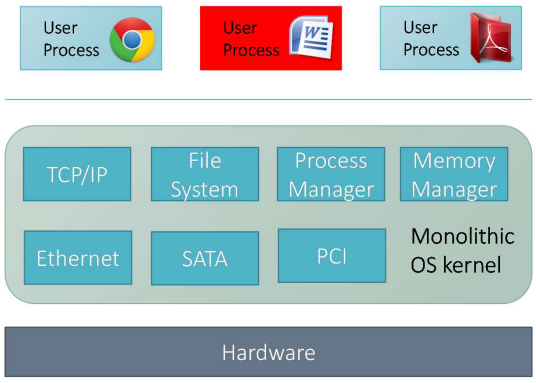

Figure 2.2: User space: Word processor hits a bug

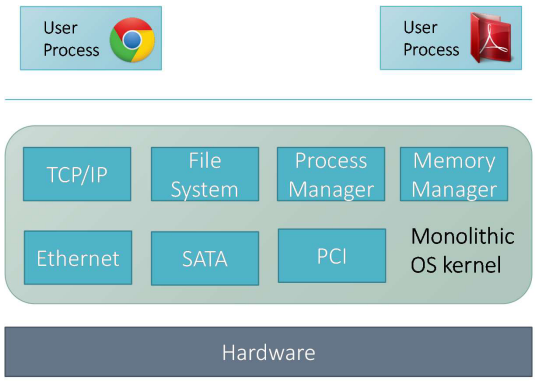

Figure 2.3: User space : Word processor crashes and system is still intact

2.1.2 kernel level

However, at kernel level, virtual to physical address translation occurs at compile-time. Run time page-table translation is not required. Since an operating system maps physical addresses directly, and also address translation is not required, memory protection policies cannot be verified at run time for every memory access. Hence, kernel components do not have memory protection similar to that of user space. At kernel level any code running at CPL 0 can access the 1 GB of kernel memory, and hence any kernel component can access and corrupt the kernel data structure.
Consider an example in below diagram.

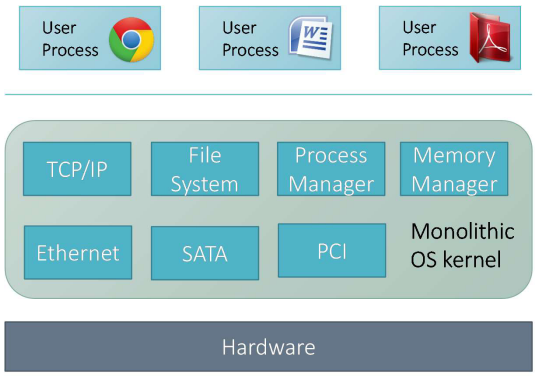

Figure 2.4: Kernel space

In the above system Chromium browser, word processor and pdf reader are running as 3 different processes in the user space and many different kernel components are running.

The network driver hits a bug, and corrupts a kernel data structure. This memory corruption might crash the other components, and might lead to a system crash.

Ideally with proper memory protection policy implementation and proper decoupling between network device driver and kernel, only network device driver and applications using network device driver (chromium in this case) should have been crashed. But because of tight coupling between device driver and kernel, complete system crashes.

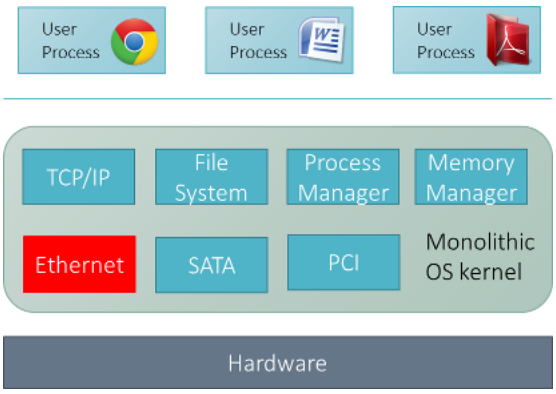

Figure 2.5: Kernel space

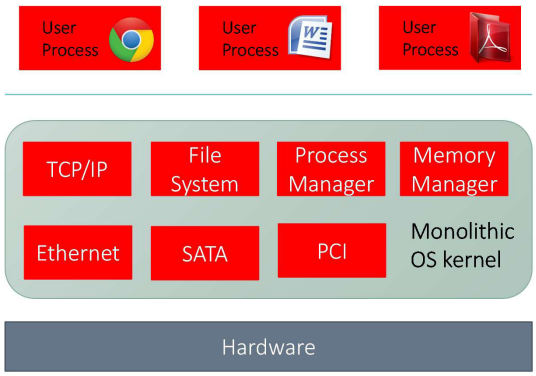

Figure 2.6: Kernel space

2.2 Virtualization

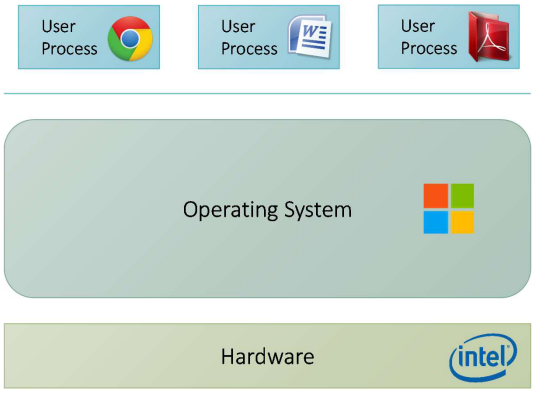

Figure 2.7: Operating System Architecture

Virtualization is conceptually similar to emulation. In an emulation, a system pretends to be another system. Similarly, in virtualization, a system pretends to be two or more instances of the same system. Originally introduced for VM/370 [12], the idea later emerged for modern platforms [8][27].

Since computer systems were expensive there was a need to share a single computer system between multiple users. This introduced the need to provide isolation between the users, which was achieved by providing the time-sharing systems. Virtualization concept started with the need to provide such isolation between users.

The addition of user and super user modes on processors protected the operating system code from user programs. A set of privileged instructions reserved for the operating system

software could run only in super user mode. The invention of Memory protection and later virtual memory made it possible to separate address spaces. The address space is assigned to different processes to share the system's physical memory and ensures that use of memory is mutually exclusive by different applications. Before introduction of virtualization these enhancements were sufficient within an operating system. But the need to run different applications and users and different operating systems on a single physical machine could be satisfied only by virtualization.[13]

Virtualization has a capability to share the underlying hardware resources and still provides isolated environment to each operating system. In virtualization each operating system runs independently from the others on its own virtual processors. Because of this isolation the failures in an operating system are contained. Virtualization is implemented in many different ways. It can be implemented either with or without hardware support. Also operating system might require some changes in order to run in a virtualized environment, or it can also function without making any changes.[15]. It has been shown that virtualization can be utilized to provide better security and robustness for operating systems[16][22][26].

2.2.1 Hypervisor

Hypervisor is a piece of computer software, firmware or hardware that creates and runs virtual machines. Operating system virtualization is achieved by inserting a hypervisor between the guest operating system and the underlying hardware. Hypervisor is also called as a virtual machine monitor (VMM).

A computer on which a hypervisor is running one or more virtual machines, is defined as a host machine. Each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. Among widely known hypervisors are Xen [5][10], KVM[19][21], VMware ESX[3],and VirtualBox[9].

There are two types of hypervisors [17]

Type 1 hypervisors are also called as native hypervisors or bare metal hypervisors. Type 1 hypervisor runs directly on the host's hardware to control the hardware and to manage guest operating systems. A guest operating-system, thus, runs on another level above

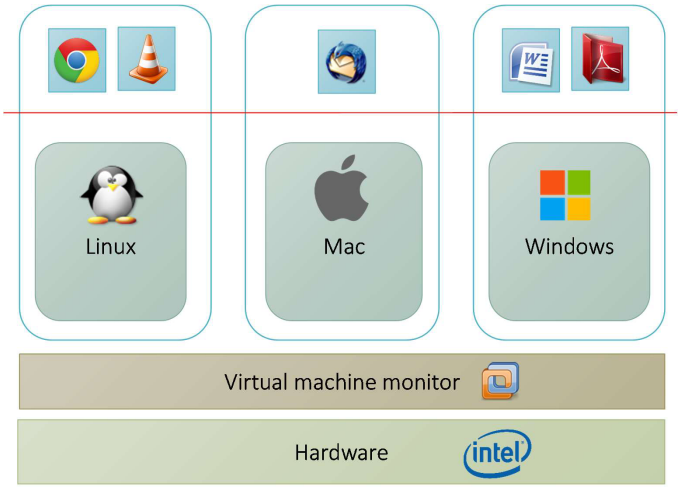

Figure 2.8: Virtualization

the hypervisor. Type 1 hypervisor represents the classic implementation of virtual-machine architectures such as SIMMON, and CP/CMS. Modern equivalents include Oracle VM Server for SPARC, Oracle VM Server, the Xen hypervisor[5], VMware ESX/ESXi[3] and Microsoft Hyper-V.

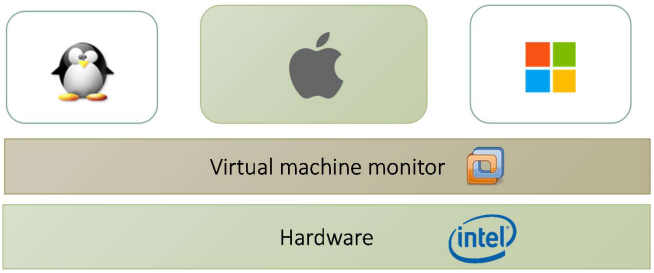

Figure 2.9: Type 1 hypervisor

Type 2 hypervisors are also called as hosted hypervisors. Type 2 hypervisor runs within a conventional operating-system environment. Type 2 hypervisor runs at a distinct second software level whereas, guest operating systems run at the third level above hardware. VMware Workstation and VirtualBox are some of the examples of Type 2 hypervisors.[30][9]

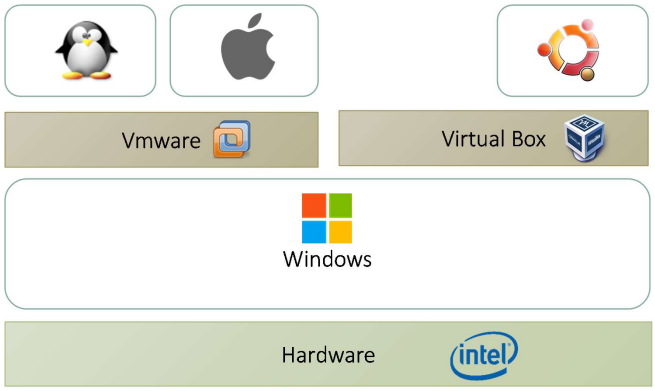

Figure 2.10: Type 2 hypervisor

2.2.2 Xen Hypervisor

Xen[5] is a widely known Type I hypervisor that allows execution of virtual machines in guest domains[20]. Figure 2.10 represents a diagram showing the different layers of a Type I hypervisor system. The hypervisor itself forms the lowest layer, which consists of the hypervisor kernel and Virtual Machine Monitors. The kernel has direct access to the hardware and is responsible for resource allocation, resource scheduling and resource sharing. A hypervisor is a layer responsible for virtualizing and providing resources to a given operating system.
Xen hypervisor does not include device drivers. In para virtualized implementation device management is included in privileged domain called as *Dom*0. *Dom*0 uses the device drivers which are present in its guest kernel implementation. Other less privileged domains called as *domU* access devices using a split device driver architecture. In the split device architecture a front end driver in a guest domain communicates with a back end driver in *Dom*0. Xen provides an inter-domain memory sharing API accessed through the guest kernel extensions, and an interrupt-based inter-domain signaling facility called event channels to implement the efficient inter-domain communication. Split drivers use memory sharing APIs to implement I/O device ring buffers to exchange data across domains.
In our implementation to isolate device drivers, we use shared I/O ring buffers in both the approaches and use event channel in the first approach.[5][23][24]

2.2.2.1 Hypercalls and events

Hypercalls and event channels are two mechanisms that exist for interactions between Xen and domains. A hypercall is a software trap from a domain to the Xen, just as a syscall is a software trap from an application to the kernel[2]. Domains use the hypercalls to request privileged operations like updating pagetables.
Event channel is to Xen hypervisor as hardware interrupt is to operating system. Event channel is used for sending asynchronous notifications between domains. Event notifications are implemented by updating a bitmap. After scheduling pending events from an event queue, the event callback handler is called to take appropriate action. The callback handler is responsible for resetting the bitmap of pending events, and responding to the notifications in an appropriate manner. A domain may explicitly defer event handling by setting a Xen readable software flag: this is analogous to disabling interrupts on a real processor. Event notifications can be compared to traditional UNIX signals acting to flag a particular type of occurrence. For example, events are used to indicate that new data has been received over the network, or a virtual disk request has completed.

2.2.2.2 Data Transfer: I/O Rings

Hypervisor introduces an additional layer between guest OS and I/O devices. Xen provides a data transfer mechanism that allows data to move vertically through the system with minimum overhead. Two main factors have shaped the design of I/O transfer mechanism which are resource management and event notification.
Figure 2.12 shows the structure of I/O descriptor ring. I/O descriptor ring is a circular queue of descriptors allocated by a domain. These descriptors do not contain I/O data. However, I/O data buffers are allocated separately by the guest OS and is indirectly referenced by these I/O descriptors. Access to I/O ring is based around two pairs of producer-consumer pointers.

1. Request producer pointer: domains place requests on a ring by advancing request producer pointer.

2. Request consumer pointer: Xen removes requests which are pointed by request producer pointer by advancing a request consumer pointer.

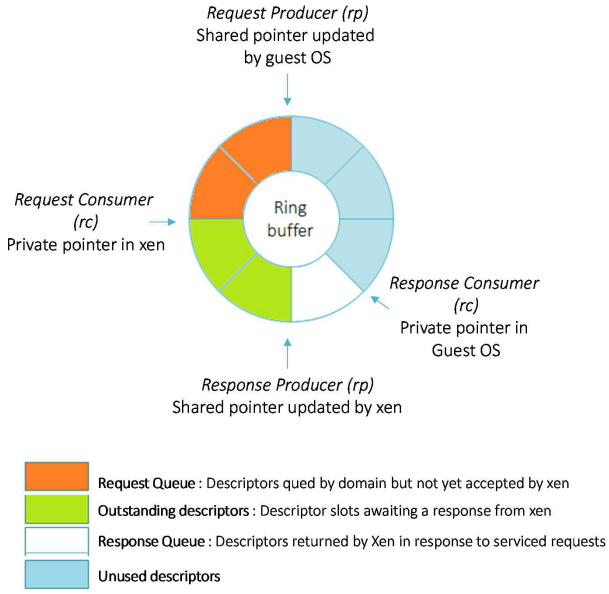

Figure 2.11: Ring I/O buffer

3. Response producer pointer: Xen places responses on a ring by advancing response producer pointer.

4. Response consumer pointer: Domains remove responses which are pointed by response producer pointer by advancing a response consumer pointer.

The requests are not required to be processed in order. I/O rings are generic to support different device paradigms. For example, a set of *requests* can provide buffers for read data of virtual disks; subsequent *responses* then signal the arrival of data into these buffers.
The notification is not sent for production of each request and response. A domain can en-queue multiple requests and responses before notifying the other domain. This allows each domain to trade-off between latency and throughput.

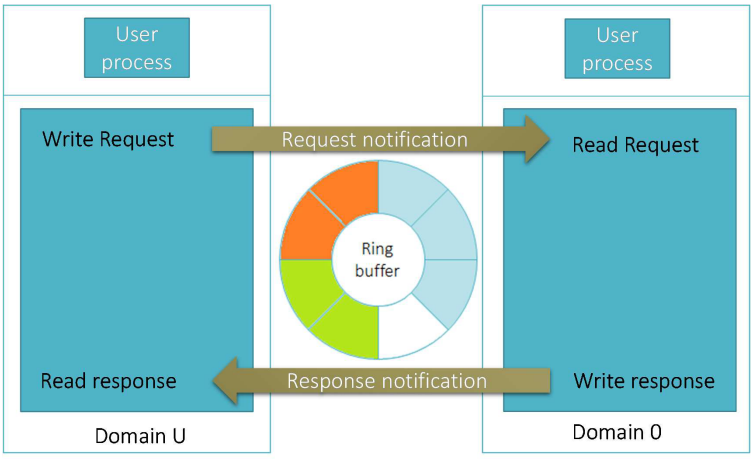

Figure 2.12: Ring I/O buffer

2.3 Processes and threads

2.3.1 Process

Process is a program in execution or an abstraction of a running program. Process can be called as the most central concept in an operating system. In early days, computer systems allowed only one program to be executed at a time. These programs had complete control of the system and hence could access all the resources of the system without any complications. However, modern computer systems allow multiple programs to be executed concurrently. To load and run multiple programs, operating system requires control over resource access and allocation. Isolation of the various programs is needed for resource allocation, which results in need of a process. A process is the unit of work in a modern time-sharing system [28].

A program is a passive entity, it is not a process by itself. Program is a file stored on disk, whereas a process is an active entity, with a program counter specifying the next instruction to execute and a set of associated resources. A program becomes a process when the file is loaded into memory[28].

A process is more than the program code, or the text section. It includes the current activity, with the help of the program counter and the contents of the processor's registers. A process generally also includes the process stack, which contains temporary data such as function

parameters, return addresses, and local variables, and a data section, which contains global variables. A process may include a heap, which is memory that is dynamically allocated during process run time[28].

2.3.2 Threads

Each process has an address space. A process has either single or multiple threads of control in that same address space. Threads run as if they were separate processes although they share the address space. [28]
Thread is also called as a light-weight process. The implementation of threads and processes differs from one operating system to another, but in most cases, thread is contained inside a process. Multiple threads can exist within the same process and share resources such as code, and data segment, while different processes do not share these resources.

2.3.3 Context Switch

Multithreading is implemented by time division multiplexing on a single processor. In time division multiplexing, the processor switches between different threads. The switch between threads is called as the context switch. The context switch makes the user feel that the threads or tasks are running concurrently. However, on a multi-core system or multiprocessor system, threads can run truly concurrently, with every processor or core executing a separate thread simultaneously.
In a context switch the state of a process is stored and restored, so that execution can be resumed from the same point at a later time. The state of the process is also called as context. The context is determined by the processor and the operating system. Context switching makes it possible for multiple processes or threads to share a single processor. Usually context switches are computationally intensive. Switching between two process requires good amount of computation and time to save and load registers, memory maps, and updating various tables.[28]

2.3.4 Spinlocks and spinning

Spin lock is one of the locking mechanism designed to work in a multiprocessing environment. Spinlocks are similar to the semaphores, except that when a process finds the lock closed by another process, it spins around repeatedly. Spinning is implemented by executing an instruction in a loop. [7]

Whenever a lock is not available, a CPU either spins or does a context switch. In a uniprocessor environment, the waiting process keeps spinning for the lock. However, the other process holding the lock might not have a chance to release it, because of which spin lock could deteriorate the performance in a uniprocessor environment. In a multiprocessor environment, spin locks can be more efficient. Overhead for spinlocks is very small, on the other hand, a context switch takes a significant amount of time, so it is more efficient for each process to keep its own CPU and simply spin while waiting for a resource. [7]

Chapter 3

System Introduction

3.1 Design Goals

3.2 System overview

3.3 System components

3.3.1 Front end module

3.3.2 Back end Module

3.3.3 Communication module

3.4 System design

Chapter 4

System Design and Implementation

4.1 Implementation Overview

4.2 Implementation

4.2.1 Communication component

4.2.1.1 Ring buffer

4.2.1.2 Shared pages

4.2.1.2.1 Hypercall interface

4.2.1.2.2 Other interfaces

4.2.2 Application domain

4.2.2.1 Front end driver

4.2.2.1.3 Initialization

4.2.2.1.4 Create request

4.2.2.1.5 Enqueue request

Chapter 5

Related Work

Related work goes here

aspos paper has good related work

5.1 Driver protection approaches

5.2 Existing Kernel designs

Chapter 6

Evaluation

6.1 Goals and Methodology

6.1.1 Goals

6.1.2 Experiment Set Up

Experiment Set Ups

6.2 System Overhead

6.2.1 Copy Overhead

6.3 Results with event channel

Results goes here

6.4 Results with spinning

Results goes here

6.5 Comparision

Chapter 7

Conclusion and Future Work

7.1 Contributions

7.2 Future Work

The idea is make the system general enough to support multiple disaster relief studies.

Bibliography

[1]

[2] hypercall. `http://wiki.xen.org/wiki/Hypercall`.

[3] Ole Agesen, Alex Garthwaite, Jeffrey Sheldon, and Pratap Subrahmanyam. The evolution of an x86 virtual machine monitor. *SIGOPS Oper. Syst. Rev.*, 44(4):3–18, December 2010.

[4] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. Xen and the art of virtualization. In *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles*, SOSP '03, pages 164–177, New York, NY, USA, 2003. ACM.

[5] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, and Andrew Warfield. Xen and the art of virtualization. *SIGOPS Oper. Syst. Rev.*, 37(5):164–177, October 2003.

[6] Victor R. Basili and Barry T. Perricone. Software errors and complexity: An empirical investigation0. *Commun. ACM*, 27(1):42–52, January 1984.

[7] Daniel Bovet and Marco Cesati. *Understanding The Linux Kernel*. Oreilly & Associates Inc, 2005.

[8] Edouard Bugnion, Scott Devine, Kinshuk Govil, and Mendel Rosenblum. Disco: Running commodity operating systems on scalable multiprocessors. *ACM Trans. Comput. Syst.*, 15(4):412–447, November 1997.

[9] Fernando L. Camargos, Gabriel Girard, and Benoit D. Ligneris. Virtualization of Linux servers: a comparative study. In *2008 Ottawa Linux Symsposium*, pages 63–76, July 2008.

[10] David Chisnall. *The Definitive Guide to the Xen Hypervisor*. Prentice Hall Press, Upper Saddle River, NJ, USA, first edition, 2007.

[11] Andy Chou, Junfeng Yang, Benjamin Chelf, Seth Hallem, and Dawson Engler. An empirical study of operating systems errors. In *Proceedings of the Eighteenth ACM Symposium on Operating Systems Principles*, SOSP '01, pages 73–88, New York, NY, USA, 2001. ACM.

[12] R. J. Creasy. The origin of the vm/370 time-sharing system. *IBM J. Res. Dev.*, 25(5):483–490, September 1981.

[13] Simon Crosby and David Brown. The virtualization reality. *Queue*, 4(10):34–41, December 2006.

[14] Peter J. Denning. Virtual memory. *ACM Comput. Surv.*, 2(3):153–189, September 1970.

[15] Ulrich Drepper. The cost of virtualization. *Queue*, 6(1):28–35, January 2008.

[16] Keir Fraser, Steven H, Rolf Neugebauer, Ian Pratt, Andrew Warfield, and Mark Williamson. Safe hardware access with the xen virtual machine monitor. In *In 1st Workshop on Operating System and Architectural Support for the on demand IT InfraStructure (OASIS*, 2004.

[17] R. P. Goldberg. Architecture of virtual machines. In *Proceedings of the Workshop on Virtual Computer Systems*, pages 74–112, New York, NY, USA, 1973. ACM.

[18] G. Scott Graham and Peter J. Denning. Protection: Principles and practice. In *Proceedings of the May 16-18, 1972, Spring Joint Computer Conference*, AFIPS '72 (Spring), pages 417–429, New York, NY, USA, 1972. ACM.

[19] Irfan Habib. Virtualization with kvm. *Linux J.*, 2008(166), February 2008.

[20] Samuel T. King and et al. Operating system support for virtual machines.

[21] Avi Kivity. kvm: the Linux virtual machine monitor. In *OLS '07: The 2007 Ottawa Linux Symposium*, pages 225–230, July 2007.

[22] Joshua LeVasseur, Volkmar Uhlig, Jan Stoess, and Stefan Götz. Unmodified device driver reuse and improved system dependability via virtual machines. In *Proceedings of the 6th Symposium on Operating Systems Design and Implementation*, San Francisco, CA, December 2004.

[23] Ruslan Nikolaev and Godmar Back. Virtuos: An operating system with kernel virtualization. In *Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles*, SOSP '13, pages 116–132, New York, NY, USA, 2013. ACM.

[24] year = 2013 Nikolaev, Ruslan and Back, Godmar, title = Design and Implementation of the VirtuOS Operating System.

[25] Thomas J. Ostrand and Elaine J. Weyuker. The distribution of faults in a large industrial software system. In *Proceedings of the 2002 ACM SIGSOFT International Symposium on Software Testing and Analysis*, ISSTA '02, pages 55–64, New York, NY, USA, 2002. ACM.

[26] Ryan Riley, Xuxian Jiang, and Dongyan Xu. Guest-transparent prevention of kernel rootkits with vmm-based memory shadowing. In *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection*, RAID '08, pages 1–20, Berlin, Heidelberg, 2008. Springer-Verlag.

[27] Mendel Rosenblum. The reincarnation of virtual machines. *Queue*, 2(5):34–40, July 2004.

[28] Abraham Silberschatz, Peter Baer Galvin, and Greg Gagne. *Operating System Concepts*. Wiley Publishing, 8th edition, 2008.

[29] Stephen Soltesz, Herbert Pötzl, Marc E. Fiuczynski, Andy Bavier, and Larry Peterson. Container-based operating system virtualization: A scalable, high-performance alternative to hypervisors. *SIGOPS Oper. Syst. Rev.*, 41(3):275–287, March 2007.

[30] Jeremy Sugerman, Ganesh Venkitachalam, and Beng-Hong Lim. Virtualizing i/o devices on vmware workstation's hosted virtual machine monitor. In *Proceedings of the General*

Track: 2002 USENIX Annual Technical Conference, pages 1–14, Berkeley, CA, USA, 2001. USENIX Association.

[31] Michael M. Swift, Steven Martin, Henry M. Levy, and Susan J. Eggers. Nooks: An architecture for reliable device drivers. In *Proceedings of the 10th Workshop on ACM SIGOPS European Workshop*, EW 10, pages 102–107, New York, NY, USA, 2002. ACM.

[32] Andrew S. Tanenbaum, Jorrit N. Herder, and Herbert Bos. Can we make operating systems reliable and secure. *Computer*, 39:44–51, 2006.