Annual ADFSL Conference on Digital Forensics, Security and Law

2008
Proceedings

Apr 24th, 3:15 PM

How Virtualized Environments Affect Computer Forensics

Diane Barrett
Associate Professor, University of Advancing Technology, Tempe, AZ, dbarrett@uat.edu

How Virtualized Environments Affect Computer Forensics

Diane Barrett
Associate Professor
University of Advancing Technology
Tempe, AZ
Dbarrett@uat.edu

ABSTRACT

Virtualized environments can make forensics investigation more difficult. Technological advances in virtualization tools essentially make removable media a PC that can be carried around in a pocket or around a neck. Running operating systems and applications this way leaves very little trace on the host system. This paper will explore all the newest methods for virtualized environments and the implications they have on the world of forensics. It will begin by describing and differentiating between software and hardware virtualization. It will then move on to explain the various methods used for server and desktop virtualization. Next, it will describe the fundamentals of a traditional forensic investigation and explain how virtualization affects this process. Finally, it will describe the common methods to find virtualization artifacts and identify virtual activities that affect the examination process.

Keywords: Hardware-assisted, Hypervisor, Para-virtualization, Virtual Machine, virtualization, VMware, Moka5, MojoPac, Portable Virtual Privacy Machine, VirtualBox,

1. INTRODUCTION

According to a research published by Gartner in February of this year, there are nearly 100 providers of products adapted for the server virtualization management marketplace [1]. Fewer than 5 million PCs were "virtualized" in 2006; by 2011, that figure will rise to between 480 million and 846 million [2].

Virtualization of both clients and servers has several attractive benefits that are fueling the use of virtual machine environments (VMEs). With more emphasis being placed on going green and power becoming more expensive, virtualization offers cost benefits by decreasing the number of physical machines required within an environment. A virtualized environment offers reduced support by making testing and maintenance easier. On the client side, the ability to run multiple operating environments allows a machine to support applications and services for an operating environment other than the primary environment.

The deployment of virtualization software is nearly a given for servers using 64-bit processors and many have built-in virtualization capabilities. However, as the use of VMEs increases, computer attackers are increasingly interested in detecting the presence of VMEs, both locally and across the network. There are some specific uses of VME technology that are driving the underground toward deploying techniques for virtual machine detection as well as an increase of virtual environments and applications that can be run from a USB device. The interest in the use and detection of VMEs is not limited to those that want to spread malware writers or conceal activities. When malicious code is released that makes use of its own VME, it will become essential for anti-malware researchers to find ways to detect the VME. Additionally, computer forensics professionals will be required to detect and examine such environments.

2. HOW VIRTUALIZATION WORKS

Is it quite complex to virtualize to an operating system. There are several published papers

explaining how virtualization works. For example, Keith Adams and Ole Agesen from VMware have written "A Comparison of Software and Hardware Techniques for x86 Virtualization". Building on this concept is "Attacks on More Virtual Machine Emulators" by Peter Ferrie. In order for virtualization to happen, a hypervisor is used. The hypervisor controls how access to a computer's processors and memory is shared. A hypervisor or virtual machine monitor (VMM) is a virtualization platform that provides more than one operating systems to run on a host computer at the same time. This section will take a brief look at the underlying technologies of virtualization.

2.1 Hardware

A Type 1 native or bare-metal hypervisor is software that runs directly on a hardware platform. The guest operating system runs at the second level above the hardware. These hardware-bound virtual machine emulators rely on the real, underlying CPU to execute non-sensitive instructions at native speed [3]. However, since they execute instructions on a real CPU, there are some changes to the environment, in order to share the hardware resources between the guest operating system and the host operating system. In hardware virtualization, a guest operating system is run under control of a host system, where the guest has been ported to a virtual architecture which is almost like the hardware it is actually running on. This technique allows full guest systems to be run in a relatively efficient manner [4]. The guest OS is not aware it is being virtualized and requires no modification. Full virtualization is the only option that requires no hardware assist or operating system assist to virtualize sensitive and privileged instructions. The hypervisor translates all operating system instructions on the fly and caches the results for future use, while user level instructions run unmodified at native speed [5].

2.2 Paravirtualization and Hardware Assist

Paravirtualization involves modifying the OS kernel to replace nonvirtualizable instructions with hypercalls that communicate directly with the virtualization layer hypervisor. The hypervisor also provides hypercall interfaces for other critical kernel operations such as memory management and interrupt handling [5].

The Virtual Machine Interface (or VMI) was developed by VMware as a mechanism for providing transparent paravirtualization. The VMI interface works by isolating any operations which may require hypervisor intervention into a special set of function calls. The implementation of those functions loads a "hypervisor ROM" [6]. This design also allows the same binary kernel image to run under a variety of hypervisors, or, with the right ROM, in native mode on the bare hardware.

Hardware vendors are rapidly embracing virtualization and developing new features to simplify virtualization techniques. In hardware assist virtualization, the guest state is stored in Virtual Machine Control Structures (VT-x) or Virtual Machine Control Blocks. Second generation hardware assist technologies are in development that will have a greater impact on virtualization performance while reducing memory overhead [5]. Both AMD and Intel have announced future development roadmaps for this technology.

Table 1 is a comparison of the hardware virtualization types as listed by VMware in "Understanding Full Virtualization, Paravirtualization, and Hardware Assist".

	Full Virtualization with Binary Translation	Hardware Assisted Virtualization	OS Assisted Virtualization / Paravirtualization
Technique	Binary Translation and Direct Execution	Exit to Root Mode on Privileged Instructions	Hypercalls
Guest Modification / Compatibility	Unmodified Guest OS Excellent compatibility	Unmodified Guest OS Excellent compatibility	Guest OS codified to issue Hypercalls so it can't run on Native Hardware or other Hypervisors Poor compatibility; Not available on Windows OSes
Performance	Good	Fair Current performance lags Binary Translation virtualization on various workloads but will improve over time	Better in certain cases
Used By	VMware, Microsoft, Parallels	VMware, Microsoft, Parallels, Xen	VMware, Xen
Guest OS Hypervisor Independent?	Yes	Yes	XenLinux runs only on Xen Hypervisor VMI-Linux is Hypervisor agnostic

Table 1: Summary comparison of x86 processor virtualization techniques[5]

2.3 Hosted hypervisors

A Type 2 or hosted hypervisor is software that runs within an operating system environment and the guest operating system runs at the third level above the hardware. The hypervisor runs as an application or shell on another already running operating system. Operating systems running on the

hypervisor are then called guest or virtual operating systems. A virtual machine monitor (VMM) provides a layer of software between the operating system(s) and hardware of a machine to create the illusion of one or more virtual machines (VMs) on a single physical platform. A virtual machine entirely encapsulates the state of the guest operating system running inside it [7]. Virtual machines are composed entirely of software and contain no hardware components whatsoever. As a result, virtual machines offer a number of distinct advantages over physical hardware.

Thus, the host can boot to completion, and launch any number of applications as usual, with one them being the virtual machine emulator. That emulator then sets up some CPU-specific control structures and uses the VMLAUNCH (Intel) or VMRUN (AMD) instruction to place the operating system into a virtualized state. At that point, there are effectively two copies of the operating system in existence, but one (the host) is suspended while the other (the guest) runs freely in the new state. Whenever an interesting event (an intercept, interrupt, or exception) occurs, the host operating system (the virtual machine emulator) regains control, handles the event, and then resumes execution of the guest operating system [3].

2.4 Embedded Hypervisors

Dell is exploring the concept of embedding a lightweight hypervisor in the firmware of some future Dell servers. Embedding a hypervisor into a system could offer a number of benefits including:

- Reducing software installation to a simple file copy
- Reducing software updates to a simple file copy
- Windows, Linux, BSD Unix and just about anything else could run simultaneously and at the same time
- Obsolete devices could appear to be present even though they've not be manufactured or supported for years
- New technology, such as hardware supporting advanced graphics, high-speed networking and storage, could be included in the system and appear to software as well-known, much loved, older devices that are compatible with generations of software [8].

The Qtopia Phone Edition demo has been designed to run in a Linux virtual machine using VMware Player and Palm OS released Garnet VM software for the Nokia series of Internet Tablet devices in November of 2007. Garnet VM is a virtual machine software application for running Garnet OS-based applications in a Linux environment that essentially acts as an emulator allowing Palm OS applications to run on a Nokia N770, N800 and N810 Internet Tablet [9]. By 2012, more than 50% of new smartphones shipped will include hardware virtualization support [10].

3. VIRTUAL TECHNOLOGY IN BUSINESS

As mentioned that the beginning of this paper, there are nearly 100 providers of products adapted for the server virtualization management marketplace [1]. IDC Research predicts that spending on virtualization will reach almost $15 billion worldwide by 2009. This section discusses some of the major players and more popular products used for virtualization.

3.1 VMware and VMware Preconfigured Appliances

Perhaps the best know virtualization vendor is VMware. VMware invented virtualization for the x86 platform in the 1990s to address underutilization and other issues, overcoming many challenges in the process [11]. VMware offers a wide variety of services and products. Of particular interest are the preconfigured appliances that can be readily downloaded and implemented using VMware Player. VMware Player makes it simple to quickly evaluate one of the many virtual appliances available through the VMware Virtual Appliance Marketplace. A virtual appliance is a pre-built, pre-configured and ready-to-use enterprise software application on a virtual machine. With VMware Player, anyone

can quickly and easily experience the benefits of preconfigured products without any installation or configuration hassles [11].

3.2 Microsoft Virtual Products

Microsoft provides a full suite of technologies to enable an integrated, end-to-end virtualized infrastructure. Using familiar interfaces and common management consoles, a virtualized environment based on Microsoft technologies simplifies infrastructure management and delivers powerful capabilities [12]. Microsoft's emphasis on virtualization technologies is rooted in creating what is called a Dynamic IT environment. Microsoft's solution includes servers, desktops, and applications virtual machine management and virtualization acceleration. Recently Microsoft has released beta versions of Hyper-V and Application Virtualization. Hyper-V provides software infrastructure and basic management tools in Windows Server 2008 that can be used to create and manage a virtualized server computing environment. Hyper-V requires an x64-based processor, hardware-assisted virtualization, and hardware data execution protection. Microsoft Application Virtualization 4.5 Beta includes new capabilities designed to aid in the support of large-scale virtualization implementations across more sites and enable multiple delivery options [12]. Microsoft has recently begun offering pre-configured Virtual Hard Disks (VHDs) that can be downloaded evaluated similar the virtual appliance market.

3.3 XenSource

Another major virtualization competitor is XenSource. XenSource distributes its hypervisor as free, open-source software but sells related products. Simon Crosby, the firm's technology chief, likens this to giving away an engine in order to sell a car around it. He believes this approach will help to spread virtualisation more quickly and prevent VMware from establishing a Microsoft-like dominance of the market. XenSource now has the necessary backing, having recently been acquired by Citrix, another software firm, for $500m. Some people think that if Microsoft fails to catch up with VMware on its own, it will buy Citrix [13]. The Citrix Delivery Center offers comprehensive end-to-end virtualization solutions, with server, application and desktop virtualization – purpose built to enable IT to deliver applications to users anywhere [14].

3.4 Parallels Preconfigured Appliances

Parallels is similar in VMware in that it provides virtualization solutions along with preconfigured appliances except for the Macintosh platform. Parallels provides server, desktop, automation and management solutions. Parallels announced the availability of a Template Catalog for Parallels Virtuozzo Containers. The company offers a library of more than 350 software downloads that can be used to easily create and manage operating systems and applications running in virtual environments [15]. The Parallels Virtuozzo Templates are comparable to VMware's Virtual Appliance Marketplace. Parallels also offers service providers access to more than 100 applications certified according to the Application Packaging Standard (APS) for software-as- a-service (SaaS) solutions.

3.5 Virtualization Boxes

Besides the above named companies, there is a wide variety of other companies that offer virtual solutions. Since the market is growing at a very fast pace, included in this section are only the solutions the author found might be relevant to the computer forensics realm.

InnoTek's VirtualBox is a mature virtualization tool that runs on Windows and Linux and supports Windows (including Vista), Linux, OS/2 Warp, OpenBSD, and FreeBSD as guest operating systems. Like many companies have done, InnoTek has split its product into two editions: An open source version and a full version with additional features aimed at enterprise customers[16]. Sun Microsystems, Inc. announced that it entered into a stock purchase agreement to acquire InnoTek in mid February of this year.

Pano Logic offers a complete desktop virtualization solution. The Pano device is a zero client. It has no CPU, no memory, no operating system, no drivers, no software and no moving parts. The Pano device connects keyboard, mouse, display, audio and USB peripherals over an existing IP network to an instance of Windows XP or Vista running on a virtualized server [17]. Pano Logic has moved the PC and all its software off the desktop and into the data center. A management device sits between the Pano device and the virtualization server.

The InBoxer Anti-Risk Appliance combines powerful email archiving, electronic discovery, and real-time content monitoring in a single appliance. The InBoxer virtual appliance separates the software from the hardware it is running on and can adopt storage virtualization [18].

4. VIRTUAL TECHNOLOGY FOR INDIVIDUAL USE

The use of virtualization is growing in the individual use market as well as the corporate environment. This section explores the technology being used with personal computer that do not alter the current environment, but use a USB device to run the virtual environment, thereby leaving the original system intact.

4.1 MojoPac

MojoPac is developed by RingCube. It now has a MojoPac enterprise solution which includes mojostation, mojodrive and mojonet. MojoPac Usher is an application that can be installed on host computers to enable MojoPac to run with a limited mode host login. MojoPac's virtualization technology encapsulates a complete Windows desktop environment, including applications, files and settings isolating it from the underlying host PC. This virtualized environment can be loaded onto a host computer, a portable USB storage device or network attached storage and run on any Windows host computer [19]. Ring Cube announced and the end of February that it has surpassed 100,000 registered users of its MojoPac software platform. This rapid adoption further demonstrates RingCube's innovative leadership in the Desktop Virtualization product category to enable users to gain greater mobility, productivity, and access to their desktops, applications, and data. "The market for portable virtual workspaces is just beginning to develop and the response to MojoPac has been overwhelming," said Pete Foley, CEO of RingCube Technologies. "To capture over 100,000 registered users in just over 1 year of the first available download for registered users validates the significant value and benefit customers have gained using MojoPac's revolutionary approach of virtualizing desktop environments and the strength of our product offering"[20]

4.2 Moka5

Moka5 LivePCs contain everything needed to run a virtual computer: an operating system and a set of applications. LivePCs can be run from a USB flash drive, USB hard disk, iPod, or a desktop computer [21]. LivePCs can be created that are similar to VMware and Parallels concept. A LivePC can be downloaded from a repository of public LivePCs created in a LivePC Library. LivePCs are run on Moka5 Engine. This technology will stream and prefetch LivePCs so they can be shared and automatically updates the LivePCs as the maintainers make changes. There is a BareMetal Edition Beta of the Moka5 Engine that is installed on a separate disk partition and the desktop computer boots directly into Moka5 Engine.

4.3 Portable Virtual Privacy Machine

The Portable Privacy Machine by MetroPipe contains a complete virtual Linux machine with privacy-enabled Open Source Internet applications. Carry your Internet applications, email, bookmarks, history, web cookies, and download files in your pocket. The Portable Privacy Machine is based on Damn Small Linux (DSL) and QEMU releases[22]. QEMU is a generic, open source processor emulator.

4.4 Preconfigured virtual appliances

VMware hosts about 725 virtual appliances that can easily downloaded and installed. Earlier it was mentioned that Parallels offers more than 350 virtual appliances. Available ready to go, are over 1,000 virtual appliances that anyone can use.

5. ADOPTION OF A STANDARD FOR PACKAGING VIRTUAL MACHINES

On November 27, 2007, the Distributed Management Task Force, Inc. created an open standard for system virtualization management "With the ever-increasing adoption of virtualization, DMTF aims to simplify and provide ease-of-use for the virtual environment by creating an industry standard for system virtualization management," said Winston Bumpus, DMTF president. "Our role also extends to ensure the success of this standard, so we are thrilled to host the first-ever SVPC plugfest to test early implementations for interoperability."[23] This standard recognizes supported virtualization management capabilities for discovering virtual computer systems, managing the lifecycle of virtual computer systems, controlling virtual resources and monitoring virtual systems.

6. HOW THESE TECHNOLOGIES AFFECT FORENSIC INVESTIGATIONS

Traditionally virtual machines have been used to create contained environments for malware isolation or to examine suspect machines. VMware can be used to mount a dd image. Applications like LiveView create a VMware virtual machine out of a raw (dd-style) disk image or physical disk. This allows the forensic examiner to boot the image or disk and gain an interactive, user-level perspective of the environment without modifying the underlying image or disk. Because all changes made to the disk are written to a separate file, the examiner can instantly revert all of his or her changes back to the original pristine state of the disk[24]. Virtual Forensic Computing (VFC) utilizes VMware's VMPlayer and the forensic disk mount tool Mount Image Pro, to re-create a subject machine in a matter of seconds. However, now instead of using virtual environments to examine machines, virtual environments themselves need to be examined.

Virtualization technology allows mobile employees to leave hardware behind and take only software with them. Entire environments can now be carried on micro devices such as a USB drive or iPod. Organizations are exploring the possibilities of downloading a virtual machine from a browser on a borrowed machine. All these technological changes present new challenges to the traditional methods of performing computer forensics.

6.1 MojoPac

MojoPac technology was described earlier. Listed below are issues that this technology presents:

- All documents and personal items can be copied to the drive, before launching.
- Once started, access to the local hard drive is eliminated.
- Access to CD and removable drives is still possible.
- May need administrative rights on the host machine in order to run.
- Currently will only run on Windows XP
- MojoPac has it’s own separate registry and shell
- Programs of the same name may be running on both at the same time
- MojoPac implements paging between memory and the hard drive to take place on the host PC instead of on the portable drive
- Process is RingThreeMainWin32
- Browsing and multimedia history stays inside MojoPac
- According to website, after a user Exits and Ejects MojoPac, there is no trace left behind on the Host PC

6.2 Moka5

Moka5 technology was described earlier. Listed below are issues that this technology presents:

- Installs VMware Player
- Asks whether you want to leave it installed for easier load next time
- Moka5 Engine will stream and prefetch LivePCs
- Any changes made during a session are captured in separate file systems on a ramdisk
- Creates folders in the my documents folder for Live PC

6.3 Portable Virtual Privacy Machine

Portable Virtual Privacy Machine technology was described earlier. Listed below are issues that this technology presents:

- Very small LINUX distro designed to boot from a USB drive
- No installation needed
- Just plug the drive into any Windows or Linux computer, and click on the Virtual Privacy Machine icon

6.4 Preconfigured virtual appliances

Preconfigured virtual appliances were described earlier. Listed below are issues that this technology presents:

- No installation needed, runs via VMware Player
- Virtual Applications can be combined. Example: BackTrack2 with Metasploit 3

7. WHAT TO LOOK FOR

In many of the aforementioned technologies, virtual devices are exclusive to the virtual machine and are files on the host. For example, VMware creates virtual adapters as well as files with extensions: .vmx, .vmdk, .vmsn., and vmss. "What Files Make Up a Virtual Machine?" posted on VMware's website is an explanation of all the files extensions that are associated with VMware along with the purpose of the file. Since some forensic software lists these extensions as unknown file types, a forensic examiner should become familiar with these files. The same goes for Microsoft's virtual products where the vhd format is utilized.

The host's critical resources such as memory, processor time, video, and sound are shared with the virtual machines. In applications such as MojoPac, the host resources must be utilized for better performance. Log files are created by most software; virtual machines are no exception, look for these. Since many of these technologies use a USB drive for access, there will be remnants in the registry. The March 2007 edition of Digital Investigation has an article titled "Tackling the U3 trend with computer forensics". Here Andy Spruill and Chris Pavan explore the artifacts left behind by U3 devices. This article is of particular interest in the investigation of virtual devices run from USB devices. When investigating virtual machines, some general items to examine include:

- MRU cache
- Link files
- Prefetch files
- Page file
- Unique identifiers associated with the program

- Artifacts in processes, file system, and/or registry
- Artifacts in memory
- VME-specific virtual hardware, processor instructions and capabilities

In the corporate environment, Application-layer security, such as application proxies can capture some evidence that can help track actions. Application-layer firewall logging can capture more than the IP address and port number. Application-layer firewalls are capable of intercepting packets traveling to or from an application such as a browser. This provides a more thorough examination of network traffic and can capture evidence from applications such as Moka5 and Portable Virtual Privacy Machine. Corporations also have the option of not allowing removable media. This can eliminate the issues that arise from using many of the technologies mentioned here.

The home environment becomes a bit more difficult. If the user is computer savvy, finding tracks may be almost impossible. Devices are becoming smaller with larger capacity and can easily be hidden. Home environments need to be examined very closely for all CDs and removable devices.

8. CURRENT CHALLENGES

A virtual machine located inside forensic software cannot currently be examined by the software. Most software reports the virtual machine files as unknown file types. Although the virtual machine can be exported or loaded into another virtual machine, when that suspect virtual machine is loaded the information inside the original virtual machine changes.

In his presentation on the Effectiveness of Hash Sets, Douglas White of the National Institute of Standards & Technology (NIST) compares physical and virtual OS installations. There is a difference in the number of files in each type of installation. His research shows the differences in physical vs. virtual machines appear to be due to devices:

- Virtual machines use abstract/generic device interfaces
- Physical machines require vendor specific drivers

This being said, any investigation now must first determine if the device being examined in real or virtual. Determining if the device is real can be done in several ways. In November of 2004, Joanna Rutkowski published the Red Pill or how to detect VMM using (almost) one CPU instruction [25]. The Red Pill focuses on detecting virtual machine usage without looking for file system artifacts based on relocation of sensitive data structures. Scoopy Doo and Jerry are tools that detect a VMware fingerprint. When Scoopy Doo is run, it simply states: This is/is not a virtual machine. These tools can be found at: http://www.trapkit.de/research/vmm/index.html. On this website, Tobias Klein also poses the question "is it possible to break out of a VM (to reach the Host OS or to manipulate other VMs)? This is quite an interesting question as the implications can be great since virtualization is based on isolated environments. For those more adventurous, Snoopy Pro is available. This tool analyzes virtual traffic between the device and driver.

When examining virtualized environments, it is important to reflect on what is being captured. Tools available to examine virtual environments are limited. The Volatility Framework 1.1.1 is a collection of tools, for the extraction of digital artifacts from volatile memory (RAM) images. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory images and provide a platform for further research into this area [26]. In May 2007 Network General added virtual server forensics. The company added modules that let IT personnel peer into the workings of VMware's ESX and Microsoft Virtual Server. However, when Henderson and Dvorak, who members of the Network World Lab Alliance, tested the virtual-machine-monitoring capabilities, they found it takes a lot of preparation and configuration work to yield useful data [27].

9. WHAT THE FUTURE HOLDS?

Virtualization appears to have a definite hold on the market and companies are competing fiercely to develop and implement products for this environment. At the end of May 2007, May Google silently acquired application virtualization startup GreenBorder. GreenBorder uses application virtualization for security containment of desktop software like browsers, email clients, and rich-media players[28]. Along with all these changes and technologies, challenges will come.

Our court system already has a difficult time with cyber crime. Earlier this year a federal grand jury issued a subpoena to MySpace.com in a case where a teenage girl committed suicide. Federal prosecutors are considering charging Lori with defrauding MySpace for creating a false account. In another recent cyber crime case, the judge ruled that there was no crime because it was a faceless crime. The judicial system is not equipped to keep up with the changing face of crime. Since virtual machines and environments are being used, can crimes committed be construed as virtual crimes? Susan W. Brenner explored the question: Is There Such a Thing as "Virtual Crime"? Her research show that the actual entry into the computer or computer system presumably occurs in the "virtual world," as would the steps an offender intends to take in order to commit an offense. This fact is not enough to prevent the liability for the offenders conduct. There is still a legally cognizable harm, such as the offender's entering an area to which she does not have lawful access and thereby violating the owner of that area's right to exclude those to whom she has not granted access. As to this fact, it is conceptually irrelevant whether the location that is unlawfully accessed exists in the physical world or in the virtual world; the harm to the owner of that area is logically indistinguishable [29]. However, the possibility of a challenge based on virtual environments still exists.

What happens when we have kiosks that a user downloads a virtual environment into a browser, commits a crime, and then deletes the virtual machine? This can happen anywhere. Virtual social networks continue to grow. How will crime be investigated in Second Life? Not long ago there were people stealing WOW gold and selling it on eBay.

In virtualization, there is the ability to roll back or delete a bad or defective machine. With the Federal Rules of Civil Procedure governing data retention, will virtual machines need to be included in an organizations data retention policy? As investigators find ways to examine virtual machines, ill the processes be questioned as to the original evidence file? Borrowing the last line from "Attacks on More Virtual Machine Emulators" by Peter Ferrie: "One thing is clear – the future looks complicated".

REFERENCES

[1] Gartner Research, The Server Virtualization Management Marketplace. Publication Date: 19 February 2008, ID Number: G00154109

[2] Gammage, B., Shiffler III, G. Report Highlight for Dataquest Insight: PC Virtualization Forecast Scenarios. Gartner Research, Publication Date: 8 August 2007 ID Number: G00150832

[3] Ferrie, P. n.d. Attacks on More Virtual Machine Emulators. www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

[4] Paravirtualization API Version 2.5. Copyright 2005, 2006, VMware, Inc. www.vmware.com/pdf/vmi_specs.pdf

[5] Understanding Full Virtualization Paravirtualization and Hardware Assist. www.vmware.com/files/pdf/VMware_paravirtualization.pdf

[6] The VMI virtualization interface. http://lwn.net/Articles/175706/ . Posted March 15, 2006 by corbet

[7] Garfinkel , T & Rosenblum, M. When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments. Stanford University Department of Computer Science

[8] Dan Kusnetzky, August 8th, 2007, Speculation about embedded hypervisors.

http://blogs.zdnet.com/virtualization/?p=205

[9] Palm OS Garnet VM Released for Nokia Internet Tablets.

http://www.palminfocenter.com/news/9526/palm-os-garnet-vm-released-for-nokia-internet-tablets/. Posted By: Ryan Kairer on Tuesday, November 13, 2007.

[10] Gartner Research, Predicts 2008: Mobile and Wireless Set New Directions in Devices and Networking. Publication Date: 17 December 2007 ID Number: G00153238

[11] VMware. History of Virtualization. http://www.vmware.com/overview/history.html

[12] Virtualization from the Datacenter to the Desktop. Microsoft. http://www.microsoft.com/business/peopleready/coreinfra/solutions/virtualization_thankyou.mspx

[13] Virtualisation. The rise of the hypervisor. Jan 17th 2008. The Economist print edition

http://www.economist.com/business/PrinterFriendly.cfm?story_id=10534566/

[14] Citrix Delivery Center. http://www.citrix.com/English/ps2/products/product.asp?contentID=683711

[15]Marshall, D. Parallels Virtuozzo Containers Offers 350 Templates. InfoWorld Virtualization Report. February 13, 2008. http://weblog.infoworld.com/virtualization/archives/2008/02/parallels_virtu.html

[16] Running, J. VirtualBox: InnoTek's virtualization goes open source

Posted Jan 15th 2007 2:45PM http://www.downloadsquad.com/2007/01/15/virtualbox-innoteks-virtualization-goes-open-source/

[17] A complete desktop virtualization solution. http://www.panologic.com/why-pano/features.php

[18] InBoxer Virtual Appliance http://www.inboxer.com/

[19]] RingCube. MojoPac http://www.mojopac.com/enterprise/products/index.html

[20] Buisness Wire. RingCube Technologies Achieves 100,000 Registered Users of Its MojoPac Virtualization Software, February 26, 2008 http://www.businesswire.com/portal/site/home/?epi_menuItemID=8529ea2ad8631dcd3bb97904c6908a0c&epi_menuID=887566059a3aedb6efaaa9e27a808a0c&epi_baseMenuID=384979e8cc48c441ef0130f5c6908a0c&ndmViewId=news_view&newsLang=en&newsId=20080226005603

[21] Moka5 LivePCs http://www.moka5.com/products/index.html

[22] The Free Portable Privacy Machine. MetroPipe http://www.metropipe.net/ppm.php?SID=4e38766ea6a3fab4792ced91b2bdbe48

[23] Distributed Management Task Force, Inc. DMTF Creates Open Standard for System Virtualization Management. http://www.dmtf.org/newsroom/pr/view?item_key=70d5d3ba78d39488626f838397a3d1e9812e5d40

[24] Live View. Carnegie Mellon University. http://liveview.sourceforge.net/

[25] Rutkowski, J. Red Pill... or how to detect VMM using (almost) one CPU instruction http://invisiblethings.org/papers/redpill.html

[26] Volatility Framework 1.1.1 (GPL). http://www.nabble.com/Volatility-Framework-1.1.1-(GPL)-td12136727.html

[27] Henderson, T, Dvorak, R. Network General tool peers inside virtual machines, Network World, 07/09/07, http://www.networkworld.com/reviews/2007/070907-network-general-test.html?page=1

[28] Google acquires application virtualization vendor. http://www.virtualization.info/2007/06/google-acquires-application.html

[29] Brenner, S.W. Is There Such a Thing as "Virtual Crime"? 4 Cal. Crim. Law Rev. 1 http://boalt.org/CCLR/v4/v4brenner.htm