Keynote

Securing Virtual Machine Monitors: What is Needed?

Paul A. Karger
IBM Corporation, Thomas J. Watson Research Center
P.O. Box 704, Yorktown Heights, NY 10598, USA
karger@watson.ibm.com

ABSTRACT

It is widely believed that the use of a virtual machine monitor (VMM) is at least as secure, if not more secure than separate systems. A recent Information Week survey [6] reports that 55% of responding business technology professionals believe that a system running in a virtual machine is as safe as physical servers and 20% believe it safer than physical servers. Such views are certainly encouraged by recent papers, such as [2] and [10]. Madnick and Donovan [9] first proposed VMMs for security in 1973 by pointing out that "since virtual machine monitors tend to be shorter, simpler, and easier to debug than conventional multiprogramming operating systems, the VMM is less error-prone."

In reality, the security of a single system running in a virtual machine can never be as secure as that single system running in its own dedicated physical hardware. The security of a system in a virtual machine depends on the correct operation of both the operating system and the hypervisor software, while in a dedicated physical computer, it depends only on the correct operation of the operating system. Because there are more lines of code that must be correct, the VMM case always has more opportunity for exploitable flaws.

What Madnick and Donovan were actually talking about was not that any one particular virtual machine was more secure, but rather that a small secure virtual machine monitor can improve the security of controlled sharing between different virtual machines, better than can a conventional operating system. The failure of any one virtual machine's operating system then can only compromise data which is accessible to that virtual machine.

While many people view virtual machine monitors as something special and different, in realty they are just special-purpose operating systems. The major difference is that the API to a virtual machine monitor is the instruction set of the virtual machine, while the API to an operating system is a set of system calls to manipulate processes, file systems, perform I/O, etc. To the extent that a particular VMM uses paravirtualization, it begins to look more like a classical operating system than a VMM.

Just like operating systems, VMMs can have exploitable security vulnerabilities. Attanasio, et. al. [1], published a classic study of security vulnerabilities in VM/370 that illustrates the problem. A more recent study of VMM vulnerabilities has been done by Ferrie [4]. Many of these vulnerabilities arise, because modern VMMs are much larger and more complex than is required. Karger and Safford [7] that not only do "modern" VMMs not meet the requirements of being small and simple, but that their approaches to I/O virtualization not only can compromise the security, but also the performance of the systems.

The solution to these security vulnerabilites is to return to Madnick and Donovan's original idea that VMMs are supposed to be very small and simple. There are VMMs that have been designed to be small and simple and to pass high-assurance security evaluations, including KVM/370 [5] and DEC's VAX VMM [8]. The only VMM to have received Common Criteria evaluation to at least the medium assurance level (EAL5) is IBM's Processor Resource/System Manager (PR/SM) [3].

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection

General Terms

Security

Keywords

virtual machine monitors, hypervisors, security kernels

ASIACCS'09, March 10-12, 2009, Sydney, NSW, Australia.

1. REFERENCES

[1] C. R. Attanasio, P. W. Markstein, and R. J. Phillips. Penetrating an operating system: A study of VM/370 integrity. *IBM Syst. J.*, 15(1):102–116, 1976.

[2] P. Barham, B. Dragovic, K. Frase, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles (SOSP)*, pages 164–177, Bolton Landing, NY, 19-22 October 2003. ACM Press. `http://www.cl.cam.ac.uk/Research/SRG/netos/papers/2003-xensosp.pdf`.

[3] Certification report for processor resource/ system manager (PR/SM) for the IBM system z10 EC GA1. Technical Report BSI-DSZ-CC-0460-2008, Bundesamt für Sicherheit in der Informationstechnik, 29 October 2008. `http://www.bsi.bund.de/zertifiz/zert/reporte/0460a.pdf`.

[4] P. Ferrie. Attacks on virtual machines. Technical report, Symantec Corporation, 2007. `http://symantec.org/avcenter/reference/Virtual_Machine_Threats.pdf`.

[5] B. D. Gold, R. R. Linde, R. J. Peeler, M. Schaefer, J. F. Scheid, and P. D. Ward. A security retrofit of VM/370. In *AFIPS Conference Proceedings, Volume 48, 1979 National Computer Conference*, pages 335 – 344, Montvale, NJ, 1979. AFIPS Press.

[6] J. Hernick. Securing VMware. *InformationWeek*, (1193):31–37, 30 June/7 July 2008. `http://www.informationweek.com/shared/printableArticle.jhtml?articleID=208801055`.

[7] P. A. Karger and D. R. Safford. I/O for virtual machine monitors: Security and performance issues. *IEEE Security & Privacy*, 6(5):16–23, September/October 2008.

[8] P. A. Karger, M. E. Zurko, D. W. Bonin, A. H. Mason, and C. E. Kahn. A retrospective on the VAX VMM security kernel. *IEEE Transactions on Software Engineering*, 17(11), Nov. 1991.

[9] S. E. Madnick and J. J. Donovan. Application and analysis of the virtual machine approach to information system security. In *Proceedings of the ACM SIGARCH-SIGOPS Workshop on Virtual Computer Systems*, pages 210–224, Cambridge, MA, 26–27 March 1973. Association for Computing Machinery.

[10] R. Meushaw and D. Simard. Nettop: Commercial technology in high assurance applications. *National Security Agency Tech Trend Notes*, 9(4):3–10, Fall 2000. `http://www.vmware.com/pdf/TechTrendNotes.pdf`.