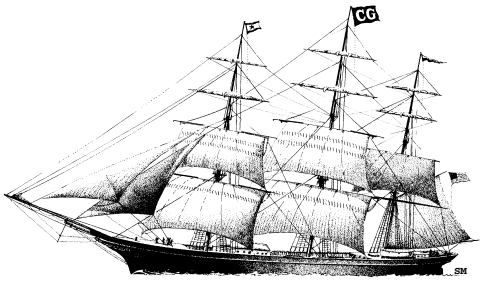
THE CLIPPER GROUP
Navigator™



Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2008031 June 6, 2008

VMware Introduces Security Technology to Make Virtualization Hosts VMsafe

Analyst: Brian J. Dooley

Management Summary

The advantages of testing a component within an environment that both isolates it and enables it to run freely have been known since ancient times. In the world of software, this concept is being applied to a variety of testing practices through virtualization. However, the idea has now been extended to the production environment, where management of virtual machines has been extended to include analysis and testing of security.

When engineers need to test machines such as engines or pumps, they install them on a testing bench, where different designs can be run and monitored at the same time without real world consequences or interference with each other. By isolating the machinery from the environment, it is possible to check all of its functions while it is running, and attach sensors to areas that would be unreachable if the machine were running alone in its normal environment. Confidence in results can be higher than in use of built-in monitoring, because internal sensors, as part of the machinery being tested, would be subject to any of its flaws, and so they cannot be trusted.

This is the strategy that has just been announced by VMware, currently the dominant player in the server virtualization area. It's new technology, called *VMsafe*, is designed to take maximum advantage of the isolating capabilities of virtualization and get at malware such as viruses, trojans, keyloggers and the like, from the outside rather than from within. **Instead of running antivirus within the machine at the same level as other software – and the malware itself – VMware proposes that that protection products should run outside the guest virtual machines, in a separate space on the virtualization hypervisor.** Like the sensors in our workbench analogy, these protection products could not only reach areas that would be invisible to internal detection, but they would also be immune to corruption from the environment, since they do not run within the infected machine. Where the test bench analogy breaks down is actually at an important part of the VMsafe offering. Unlike the test bench, the monitored machines may be performing their real world functions even while they are being monitored and tested, because isolation from the environment is sufficient to ensure that problems within the guest machine cannot leak out to affect other guest machines. Thus, there is no reason to bring processing to a halt while a guest machine is being examined, because monitoring is external to that machine.

VMware is offering its VMsafe technology as a set of APIs that can be used by vendors of protection products to reach into virtual machines and locate problems. This is a logical extension of its own virtual machine management portfolio, but it takes the added step of involving the companies that have specialist expertise in malware identification and containment. The company is working with partners representing most of the top names in the security field to provide trusted products capable of operating within this sphere. It is using a partnership program rather than supplying API access outright so that it can control who can enter the privileged realm of virtual machine hosting. Control of this aspect will be important to ensuring that the environment itself remains secure. Read on for more details.

IN THIS ISSUE

The Technology

The VMsafe technology offers transparent access to memory, CPU, disk, and I/O systems of hosted virtual machines, and provides capability to monitor all operations on each system. Security products that are using the VMsafe APIs will be able to stop malware before it is able to do harm, and will also be able to reach, identify, and eliminate numerous types of threats, such as rootkits, which are hard to detect or undetectable on physical machines.

So far, 20 security vendors have announced plans to use the *VMsafe* APIs, including McAfee, Symantec, Sonicwall, Trend Micro, Checkpoint, Tripwire, and EMC's RSA division. Partners will be supported with pre-release access to the APIs, a certification program, joint marketing initiatives, and use of the VMsafe logo.

For VMware, VMsafe is part of an evolutionary movement from current concerns over securing virtualized environments, to a point where virtualization is a key component of security infrastructure. The first step has been to secure the core virtualization products and components. The next step is to extend the reach of existing security products to virtualized environments. The final step is to provide "unique security through virtualization" in which current security products based upon the physical machine become obsolete.

Virtual Machine Security

As virtualization has become an increasingly important reality in today's computing infrastructure, it brings about numerous changes from operations on standalone systems. Areas that need to be addressed include issues of availability, backup, security, authentication, patching, and auditing of hosted systems.

Network management, security, and data protection have all evolved in a world of discrete machines in which inter-machine communication is along physical routes that can be easily monitored and controlled. This is particularly important in security, where intrusion detection systems (IDS) have operated as an important safeguard.

Relatively few network management and monitoring tools are (yet) ideally suited to securing guest systems in a virtual environment, where machine-to-machine communications may occur within the host rather than through standard network devices. Most current network defenses have been built upon a concept of "seeing" the traffic. Unless some provision is made for this, the commonly accepted defenses cannot be readily applied. A number of virtual environment security tools exist, but this area is in an early state of development.[1]

The first step in virtualization security was to secure the environment itself. The hypervisor operates at a privileged level, and is capable of affecting the behavior of the machines that it hosts. If the hypervisor should ever be compromised, it could, in theory, yield access to all of the hosted servers – which might include several hundred.

Securing the hypervisor has so far proven less difficult than feared. First, hypervisors are small pieces of software, and they have a smaller "attack surface" than operating systems. A great deal of control can also be exerted over client access and control. Protection has been added by incorporating the Trusted Computing Group's Trusted Platform Module (TPM) standard to provide hardware-based security support. TPM helps to detect and prevent tampering. In virtualization, it makes sure the hypervisor itself is loaded in a trusted state, therefore making it difficult to compromise. Other technologies, such as memory hardening, update and patch management, and a range of internal tools have been applied. **However, it has become clear that virtualization itself could be used as a part of the solution, and is actually capable of providing overall improvements in the security environment, once its own security issues had been addressed. VMsafe is the next logical step.**

VMware's security solution is to provide APIs that will enable companies that have long provided security on a conventional individual machine or network basis. This will let them create products to "see" into operations and communications between virtual machines, thus making it possible to apply their tested technology to the new environment. The result should be a seamless security fabric that includes equivalent measures and procedures across both physical and virtual systems and communications components. An important aspect of this concept is that it will encourage development of a holistic approach, rather than creating security silos across the enterprise, with one security system operating in the virtualized universe, and another system operating in the physical universe. Although there will be differences in the way detection is carried out, the major security vendors have

[1] Vendors include Blue Lane Technologies and Reflex Security.

already signed up to embrace VMsafe, and it is likely that they will deliver products that integrate into their existing management schemes.

VMware's 20 announced partners for VMsafe provide a wide range of security services, ranging from intrusion protection to antivirus solutions. Since the initiative has only just been announced, it is hard to tell what the final result will be. **For VMware, however, it shifts the spotlight from concerns over security within a virtualization environment to the possibility of leveraging that environment to improve overall security.**

Conclusion

VMsafe is a new security initiative in the virtualization sector that deserves attention for several reasons. First is its industry support. VMware is the dominant force in the virtualization sphere, and this effort enlists most of the major players in the security industry, aiding them to bring their products within the hosting environment. Second, it moves beyond simply securing the hosting environment toward an extended vision of security. It is this vision that provides the unique element. The idea is to use the isolation afforded by virtualization as a means of strengthening security. Not only will partners be able to extend their products into the host environment, but also they will be able to develop strategies for securing virtual machines and their applications less intrusively, more efficiently, and more effectively than can their counterparts on individual physical servers.

This vision fits very well with VMware's overall vision of ubiquitous virtualization. The connections can be secured between hosting environments, but most of the security operations will take place within hosting systems, operating out of virtual machines taking advantages of the special privileges offered by the VMsafe APIs.

As virtualization has spread through organizations, security and administrative solutions that are specifically designed to work with and within a virtualized environment are becoming increasingly important. This is an area that you cannot afford to ignore, and that will demand even greater attention in years to come.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Brian J. Dooley **is a Contributing Senior Analyst for The Clipper Group.** He has more than 25 years experience as an author, analyst, and journalist focusing on IT trends. He has written six books, numerous user manuals, hundreds of reports, and more than 2,000 magazine features. Mr. Dooley is the founder and past president of the New Zealand chapter of the Society for Technical Communication. He initiated and is on the board of the Graduate Certificate in Technical Communication program at Christchurch Institute of Technology. Mr. Dooley currently resides in New Zealand.

- ***Reach him via e-mail at bj.dooley@clipper.com.***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group** *Captain's Log*, **The Clipper Group Voyager,** *Clipper Notes*, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.