Virtual Security: The New Security Tool?

James Tiller

In 1996, I found a tiny package floating around the Internet called VMware. I booted up my Linux laptop and proceeded to install this little animal. Within minutes I started the application and booted my first virtual PC. Compelled to investigate further, I decided to load Windows 95, completely convinced that it would fail miserably — Win95 on Linux, are you kidding me? To my surprise, I was browsing the Web using IE, in Windows 95 from a virtual PC running on Linux in just a few hours. Little did I know at the time that virtualization would make the huge rebirth that it has today.

Rebirth seems like the appropriate word. Anyone familiar with IBM and Tandem, to name a couple, are familiar with virtualized computing. But these solutions fell victim to the distributed computer resource model emerging in the late 1980s and in full bloom in the mid-1990s. By the time I was introduced to VMware it seemed almost out of place and time, an oxymoron with seemingly little value when piles of servers were the answer and technology was the key business enabler. But today it’s not about the technology — it’s about services — IT and security services mapped to business drivers, making technology transparent to the mission. It is within this framework and IT business management evolution that virtualization was reincarnated.

My first Internet page hadn’t finished loading in my Win95/Linux system when the thought of security chilled my spine. At that time I was enamored by trusted operating systems (TOS). The thought of compartmentalization from the NIC to the applications, and everything in between, was, for me, security nirvana. I was an Argus PitBull, Solaris TOS, and HP Virtual Vault bigot; I was convinced TOS was the future. Now with virtualization, compartmentalization was holistic, fully encompassing my environment, an environment I could manipulate, adjust, specialize, and distribute seamlessly. My TOS convictions began to waver.

Today, virtualization has many solutions. VMware, now part of EMC, is locking horns with Microsoft. With virtualization part of Longhorn, it is clear that giants are making big bets, and so are some of their customers. Virtualization appears to many executives as the ultimate money press, squeezing every last cycle from the pools of vast underutilized resources. All this in the midst of data center consolidation and cost sensitivity that has catapulted virtualization to the boardroom and the CIO’s desktop.

Once I was familiar with the Win95/Linux Frankenstein I had created, I began to investigate the security attributes. At that time ISS’s system scanner was embryonic, but made for a good starting point to run a scan. Starting from a remote system on my home network and then moving my attack source point to the host Linux system, I
found what one would expect, the typical holes found in default installs. But what of the internal interactions? Having dabbled in TOS, I felt I knew where to poke around. After several days led to weeks, only the system memory presented an option for a broad attack — an attack that would essentially offer multiple system access with one swing of the bat. A well-constructed worm or sophisticated tool could take advantage of the overlap. It needed further research.

Anyone with a PC can download Microsoft’s Virtual PC and load multiple virtual machines on their computer. The same holds true with VMware. On one hand, I’m very excited about the opportunities this offers; on the other, it is terrifying.

Think of all the interesting possibilities with virtualization, beyond just saving money and reducing cost — which are extraordinarily convincing and intoxicating for the CFO. Entire systems can be provisioned with an e-mail. In minutes you have a server configured exactly how you need it, ready and awaiting your command. When you’re done, you delete your system. No more reallocation of assets, product lifecycle management, decommissioning woes, budget battles, and business units trying to crush the CIO because their new marketing server is still in parts on the data center floor.

Business continuity takes on new meaning. Applications are ignorant of the system, a system that can be anywhere on any hardware. CPU cycles can be handed out in tiny packages. Memory and storage are controlled and allocated on demand. Quality of service has migrated from the network into the silicon.

Think of the impact to emerging technologies and those that have yet to be fully embraced. IPv6 is one of the few that may become a requirement and not a luxury in the very near future. Virtualization can be the migration path for applications — even networks and storage (no wonder EMC bought VMware). Service Oriented Architectures in application development will map to virtual profiles and not the system you install it on.

But what of security benefits? Think of consolidated labs where near real-time systems can be tested for vulnerabilities and patches can be verified in minutes with no risk to production systems or data. Standard systems builds can be changed more readily, deployed more quickly, and applications simply moved over with no or much reduced downtime. Entire DMZs may become a single computer cluster with dedicated virtual systems for each service. Images of systems can be provided to vendors to perform penetration tests and application tests at no risk and no concern over hardware. The emergence of virtual system policies is inevitable. Analogous to group policies in Microsoft environments, system policies will govern every attribute of the virtual computer from system attributes, to drivers, to operating system, to services, and to applications. The list goes on because the simple act of separating the system from a physical device implies greater control with faster results. Entire computer systems are now files that can be replaced rapidly with hardened versions and the business applications are none the wiser, just more secure.

But what of the security risks? Is it not obvious? Take the simple fact that if some organizations cannot employ good security practices for their existing collection of computer resources, does this not imply that the same would hold true for ten times the number of computers? Forget the fact they are virtual; they are nonetheless computers unto themselves. The vast number of possibilities for leveraging this deceptively simple technology for advanced security management at the system level is, in a nutshell, worthless to those without meaningful processes and progressive thinking. Without a quantum shift in security strategy and willingness to adapt quickly, virtualization will consume the CISO, exploiting every weakness in the program through shear numbers.

The voracious appetite for systems in the business units will be unleashed on a smorgasbord of virtual systems. Automated provisioning will spread like wildfire and
whatever existing security practices are in place will be equally replicated — for better or for worse. Were you ravaged by SQL-sammer because you had 300 SQL servers and MySQL running on unaccounted systems sitting under the desks of your development division? If you have a hard time keeping the reins on rogue systems now, multiple that by a hundred today, a thousand in a year. How do you manage system security when systems appear and disappear in weeks, days, or hours? Waves of vulnerable systems will replicate in minutes across your environment, instantly changing your defensive profile. Your exposure to multiple threats, such as worms, may materialize and vanish in days before you have a chance to react — all without the knowledge of when it may surface again. Incident response will be a constant activity and risk visibility will be clouded by a sea of change. It could be chaos.

From a technical perspective, the dynamics of the technology are so great that it is difficult to understand fully the security controls that exist within the supporting kernel of a host system. The need for loading an operating system, then virtualization software, and then virtual systems is already “old school.” What was once hardening the base operating system to provide a secure foundation for the virtual systems is migrating to smaller, specialized kernels that will need to be tested from all perspectives.

It is understanding the interactions between the virtual systems, ironically, at the abstraction point between the hardware and the underlying code that will become critical. This will be an enormous challenge and one can expect the emergence of tools specifically designed to test the lower levels of system operations that support an array of virtual computers.

Nevertheless, the previous statements are directed at the server environment and the thought that the base operating system security will be the weakest link that translates to the virtual system security remains valid for the numerous desktops that will happily consume the technology.

CISOs must fully embrace virtualization and all that it implies. Although understanding the technical attributes and nuances is important for your security team, it is the philosophical application of the technology that must be investigated and turned on its head. Do not try to absorb the energy exerted from above in an attempt to keep pace; you will fail. Endeavoring to stem the tide will only position security, once again, as the disabler to business evolution — again seen as Cerberus the gatekeeper and not the mindful protector of growth and expansion. Security groups must develop methods for leveraging the same features that make virtualization valuable to the CIO for the betterment of security. This is not putting in policies and solutions that inhibit adoption; it is the full and complete assimilation of the ethereal characteristics from a security perspective.

The first step in preparing for the inevitable is process evolution. Review the security plans and processes, roles and responsibilities, policies and governance and apply them as if empowered by virtualization. Clearly, an information security management system and process improvement framework must exist to allow a comprehensive sandbox approach. Nevertheless, attack the issue from the perspective that virtualization will become the next security tool and not as yet another disruptive technology that will be forced upon the security group to support and manage.

As the weeks turned to months, my Win95/Linux system — then affectionately name Igor — received less and less of my attention. It was a Linux tool when Linux was less understood and long before its proliferation into the mainstream. Few discussed it and fewer seemed to be using it. With that it fell into obscurity, residing with the multitude of other little animals that I played with on occasion. Little did I realize that I was staring into the eyes of what would become a beast.

Whether or not it becomes a security beast of burden is ultimately up to you and your imagination.