Technology | DOI:10.1145/1467247.1467253 Kirk L. Kroeker

The Evolution of Virtualization

Virtualization is moving out of the data center and making inroads with mobile computing, security, and software delivery.

IT'S NO SECRET that virtualization, a technology long associated with mainframe computers, has been transforming data centers due to its ability to consolidate hardware resources and reduce energy costs. But in addition to its impact on data centers, virtualization is emerging as a viable technology for smartphones and virtual private networks, as well as being used to reconceive agile and cloud computing.

Over the past decade there has been a great deal of work on improving the performance, enhancing the flexibility, and increasing the manageability of virtualization technologies. Developments in the past five years alone, for example, include the ability to move a running virtual machine, along with its live operating system and applications, to a physical host without major downtime. The industry has also recently witnessed the ability of virtualization to log the actions of a virtual machine in real time, with the purpose of being able to roll back an entire system to an arbitrary point and then roll it forward for debugging or auditing. These and other recent developments have positioned virtualization as a core technology in cloud computing and have facilitated the technology's move to the desktop.

"It's clear that virtualization is here to stay," says Steve Herrod, chief technology officer at VMware. "In the future, we'll look back at the nonvirtualized compute models as we look back at the phonograph and bulky CRTs." But Herrod also says that the industry is far from realizing the full benefits that virtualization can bring to desktops, laptops, and smartphones. "Virtualization is picking up steam rapidly for desktop users, but it has certainly not achieved ubiquity yet," he says. "End users don't want or need to know that virtualization is being used; they want access to their applications, and they want the very rich media experiences that many modern applications offer."

An iMac computer, with VMware Fusion, which enables it to run Windows XP Pro on the left screen, Windows Vista Home on the right, and Mac OS X Leopard in the background.

Arguably, one of the most interesting and novel uses of the technology is on mobile devices, where virtualization enables several new use-cases, such as isolating work and home smartphones on a single physical handset. Gartner predicts that more than 50% of new smartphones will have a virtualization layer by the year 2012. The need for virtualization on smartphones is strong, says Herrod, particularly as these devices become more powerful, as mobile applications become more advanced, and as security becomes a bigger issue. "Just as in the early days of our x86 desktop virtualization efforts, we see many different benefits that will come with this virtualization," says Herrod.

As one example, Herrod cites the substantial testing procedures that every new handset must undergo prior to shipping. Virtualization, he says, will let handset manufacturers test once and deploy on different handsets. For the carriers, Herrod predicts that virtualization will enable a new set of services, such as allowing users to deploy a virtual copy of their mobile data to a newly purchased handset. And for businesses, he says that those who want a single handset for home and work will be able to use different virtual phones. "Their work phone could be restricted to very specific applications and corporate data that is secure and completely isolated from their home phone, where they may have personal information and games," he says. "The more we talk with people about this new area, the more use-cases we find."

Enhanced Security

The notion that one of the strengths of virtualization is its ability to isolate data and applications corresponds to another aspect of the technology

SCREENSHOT BY CHRISTOPHER GLISSON

that has become increasingly popular. While it might be easy to think of virtualization as adding a software layer that requires additional controls to maintain security, proponents of virtualization argue that it serves the opposite purpose, and instead represents a core enhancement to security. "The only way we know how to get strong isolation is to keep things simple," says Mendel Rosenblum, founder of VMware and a professor of computer science at Stanford University. "And the only way we know how to do that is to have isolation enforced at the lowest level."

Modern operating systems have a high level of functionality—and a corresponding level of complexity and number of potential weaknesses. "I look at virtualization as a step toward getting out of the mess we have in terms of these systems being so insecure," says Rosenblum, who maintains that better security is a natural result of virtualization. Still, he says, it is incumbent on those working on virtualization to build layers that don't make virtualized systems so full of features and complex that they become difficult to secure.

Ian Pratt, founder of XenSource and vice president of advanced products at Citrix, has a similar view of virtualization's relationship to security. "If you look at hypervisors for laptops and phones, it's not about consolidation," he says. "It's about security and being able to secure different partitions on a device."

Citrix is developing software for a model of mobile computing that the company calls "bring your own computer," with the idea being for employees to use their own laptop for securely connecting to the corporate network. In this model, the laptop runs a corporate virtual machine directly on top of a hypervisor rather than in a hosted virtual environment contained by the employee's personal operating system.

"You need to provide very strict isolation between those environments because you really don't trust the personal environment," says Pratt. "It is only through using a hypervisor where you can achieve that strong isolation between those environments."

Like VMware's Herrod, Pratt points to smartphones as one manifestation of this new way of thinking about virtualization and security. In Pratt's example, a handset might have one virtual machine that controls the radio, another that contains all the default software and applications, and a third that operates everything the user downloads and installs. "The whole idea behind this," says Pratt, "is that because you have this strong isolation, no matter what rubbish you download and install on the phone, you are still going to be able to make that 911 call whenever you need it."

With virtualization, people will be able to use both their work phone and home phone on a single handset.

Proponents of virtualization say that, in addition to facilitating new ways of enforcing security, virtualization technologies are leading to new ways of distributing software. "Virtualization not only gives you the ability to manage hardware more effectively," says Rosenblum, "but also allows you to treat the software you're running differently." One way of leveraging virtualization's capabilities is to ship complete packages of running virtual machines rather than having users assemble operating systems and applications themselves, he says. The idea represents a different take on software as a service, a model that obviates the need for users to assemble applications themselves. "It's not like you buy all the separate parts to make a car, but that's what we do with computers," says Rosenblum, who predicts that virtualization will lead to users simply invoking complete, authenticated virtual machines tailored to their particular needs.

Core Challenges

While virtualization is continuing to make inroads in several new areas and

Quantum Computing

Atoms Teleported

A team of scientists from the University of Maryland and the University of Michigan have successfully teleported information between a pair of atoms, housed in separate and enclosed containers, across a distance of one meter, reports *Science*. According to the scientists, this is the first time that information has been teleported between two separate atoms in unconnected containers.

With their protocol, the scientists successfully teleported quantum information between two ytterbium ions, using a method of teleportation in which the ions are stimulated to emit photons and the quantum states are inferred from the color of the emissions. The scientists report that atom-to-atom teleported information can be recovered with perfect accuracy approximately 90% of the time, and they believe that figure can be improved.

"Our system has the potential to form the basis for a large-scale 'quantum repeater' that can network quantum memories over vast distances," says Christopher Monroe, the team leader and a physics professor at the University of Maryland. "Moreover, our methods can be used in conjunction with quantum bit operations to create a key component needed for quantum computation.

"One particularly attractive aspect of our method is that it combines the unique advantages of both photons and atoms," says Monroe. "Photons are ideal for transferring information fast over long distances, whereas atoms offer a valuable medium for long-lived quantum memory. The combination represents an attractive architecture for a 'quantum repeater,' that would allow quantum information to be communicated over much larger distances than can be done with just photons. Also, the teleportation of quantum information in this way could form the basis of a new type of quantum Internet that could outperform any conventional type of classical network for certain tasks."

is leading to speculation about new models of computing, the technology's overhead remains a core challenge. Recent advances in hardware and software have been removing some of the performance concerns associated with virtualization, but the goal is to eliminate the performance gap altogether. "We are not there yet, but what you're going to see is enhancements in processors and other technologies to make the performance gap go away," says Leendert van Doorn, who is a senior fellow at AMD and responsible for AMD's virtualization technology, including the AMD virtualization extensions in the company's latest quad-core Opteron processor, which are designed to reduce the performance overhead of software-based virtualization. "The big problem with virtualization right now is performance guarantees," he says. "If you have a database transaction requirement of a few milliseconds, it is very difficult to provide that guarantee in a virtualized environment."

Still, van Doorn says he is confident that this overhead will be reduced in the coming years with better hardware and software support for virtualization. Currently, overhead in virtualized environments varies from a few percent to upward of 20%, a figure that van Doorn says depends on several factors, including how the hypervisor is implemented and whether the operating system running atop the hypervisor is aware that it is being virtualized. "The Holy Grail is to get near-native performance," he says. "We are getting closer to that goal."

In the future, all new machines might have virtualization capabilities embedded in their firmware.

In addition to the performance issue, there remains the issue of manageability in the data center and elsewhere. "For the next generation, every big software company is working on comprehensive management tools," says van Doorn. The goal is to deal with a massive number of virtual machines and effectively make global optimization decisions for thousands of virtual systems running in data centers or in the hands of a large work force. Sophisticated management tools will be essential in the future imagined by virtualization's proponents, who predict that industry is moving toward a world in which the technology is ubiquitous, and where all new machines will have virtualization capabilities embedded in firmware.

Certainly, says Citrix's Pratt, all servers, desktops, laptops, smartphones, routers, storage arrays, and anything else running software that must be isolated from other applications will be virtualized. The result? "The main noticeable thing will be more trustworthy computing," says Pratt. Echoing this sentiment, Herrod predicts that users won't think about virtualization as a different form of computing. "It will seamlessly fit into our notion of computing," he says, "enabling a much simpler and more productive experience for all of us." C

Kirk L. Kroeker works in communications and has written extensively about the impact of emerging technologies.
Steven Hand, Citrix, and Carl Waldspurger, VMware, assisted in the development of this article.

Obituaries

In Memoriam

The world of computer science recently lost two esteemed members: Oliver G. Selfridge, who died at 82, and Ingo Wegener, 57.

Selfridge, whose career included positions at MIT,

BBN, and GTE Laboratories, is widely regarded as a leading pioneer in the field of artificial intelligence and the father of machine perception. "In prescient research in the 1950s," says Eric Horvitz, president of the American Association of Artificial Intelligence, "he introduced and tackled key problems that are now well known to machine learning researchers, including the challenges of search and optimization over large parameter spaces, feature definition and selection, dependencies among variables, and unsupervised learning—learning without explicit access to signals about success versus failure."

In 1956, Selfridge, with four colleagues, organized a conference at Dartmouth College that led to the creation of the field of artificial intelligence. And his 1958 paper, "Pandemonium: A Paradigm for Learning," is a classic AI treatise that essentially provides a blueprint for machine learning research.

"The Pandemonium work introduced a distributed model for pattern recognition, where a community of interacting 'demons' or agents with different competencies and functions perform different subtasks that are then combined into final answers or behaviors," Horvitz notes. "Rather than being handcrafted ahead of time and fixed, the agents and their networks of communication could evolve with experience.

"For decades, Oliver communicated an exciting vision where computers would one day learn to infer human intentions and act to assist people without the need for detailed expression of problems," says Horvitz. "Such a vision has evolved to be central in research on human-computer interaction."

Ingo Wegener, a professor of computer science at the Technical University of Dortmund, is well known for his groundbreaking work in complexity theory. He wrote a pair of important monographs, *The Complexity of Boolean Functions* (1987) and *Branching Programs and Binary Decision Diagrams* (2000). In the early 1990s, he worked in the formal analysis of metaheuristics, and his conviction that optimization algorithms based on metaheuristics, like evolutionary algorithms and simulated annealing, should be studied with the methods from

the theory of efficient algorithms and complexity theory. Wegener's new, theoretical approach produced a profound understanding of the limitations of such metaheuristics.

Wegener was appointed a member of the German Council of Science and Humanities, the leading scientific advisory committee to the German government, in 2004, and won the Konrad-Zuse-Medal, Germany's most prestigious computer science award, in 2006.

LEFT: PHOTOGRAPH COURTESY OF CAROLINE SELFRIDGE. RIGHT PHOTOGRAPH COURTESY OF INFORMATIONSDIENST WISSENSCHAFT