

# SECURE HYPERVISOR

IT resources are a significant investment for modern businesses. Servers are expensive and power hungry, the management and support of the systems is complex and security is a constant concern. However, initiatives such as the open-source Xen virtual machine monitor are changing this.

A decade ago computer scientists at the University of Cambridge set out to rethink the traditional computer server model. As one of the faculty members at the time Ian Pratt revealed, "We were interested in how to make computing more like a utility where users could buy some secure computer time as a service." The solution was a virtual machine monitor, or hypervisor, that the researchers called Xen.

Virtualisation, where computers are divided up into several virtual machines with their own operating systems and applications, is not new. IBM began working on this concept 40 years ago to improve computing performance.

However, Xen has some advantages over other approaches that have enabled it to become widely used by major computing companies around the world. "We try to

keep the core hypervisor as small as possible and push everything else out to virtual machines providing services. Other approaches are more monolithic in their architecture," explained Pratt.

"Xen is designed with isolation in mind," he continued, pointing out that fierce rivals such as Coca-Cola and Pepsi could confidently have their processes running on the same physical machine without risk of their corporate information being accessed by their competitor.

The Xen hypervisor was launched in 2002 under an open-source model. In 2004, the Cambridge research team set up a company, XenSource, to offer enterprise versions. This company was acquired by Citrix in 2007 and Xen is now built into products from many major companies, including Oracle, Dell and HP, as well as Citrix.

Parts of Xen are built using OCAML, a modern, compiled, functional programming language. "We wanted to build a system that was robust, reliable and secure," said Pratt, who is now Vice President for Advanced Products at Citrix. "Good developers can learn OCAML very quickly and that's the kind of developers that we want to attract to the community."

The open-source community plays an important role in the ongoing development of Xen. "Chipmakers like Intel and AMD really know how to make Xen work well on their chips because they developed them," said Pratt. "They talk to us about potential developments long before they begin to be fabricated in silicon, so new chip features are created with Xen in mind." Similarly, Oracle's involvement ensures that Xen works with its databases.

There are twice-yearly developer meetings and several hundred developers submit code to the project. The latest release, Xen 4.0, includes around 20,000 updates since the previous major release. Xen is also at the forefront of the recent moves into 'infrastructure as a service' cloud computing, where many physical machines running hypervisors are connected together into resource pools and virtual machines dynamically allocated across them.

This approach enables computing resources to be optimised for power and performance. When there is less demand, perhaps at night, the virtual machines can be consolidated down on to some smaller number of physical servers, enabling the other servers to be powered-down. The hypervisor can also provide high-availability and even hardware fault tolerance for mission critical applications.

Further information:  
[www.citrix.com](http://www.citrix.com)  
 and [www.xen.org](http://www.xen.org)

