

# Making operating systems safer and faster with 'unikernels'

January 28 2016, by Sarah Collins

---



Technology to improve the security, speed and scale of data processing in age of the Internet of Things is being developed by a Cambridge spin-out company.

Specialised computer software components to improve the security, speed and scale of [data processing](#) in cloud computing are being developed by a University of Cambridge spin-out company. The

company, Unikernel Systems, which was formed by staff and postdoctoral researchers at the University Computer Laboratory, has recently been acquired by San-Francisco based software company Docker Inc.

Unikernels are small, potentially transient computer modules specialised to undertake a single task at the point in time when it is needed. Because of their reduced size, they are far more secure than traditional [operating systems](#), and can be started up and shut down quickly and cheaply, providing flexibility and further security.

They are likely to become increasingly used in applications where security and efficiency are vital, such as systems storing personal data and applications for the so-called Internet of Things (IoT) – internet-connected appliances and consumer products.

"Unikernels provide the means to run the same application code on radically different environments from the public cloud to IoT devices," said Dr Richard Mortier of the Computer Laboratory, one of the company's advisors. "This allows decisions about where to run things to be revisited in the light of experience - providing greater flexibility and resilience. It also means software on those IoT devices is going to be a lot more reliable."

Recent years have seen a huge increase in the amount of data that is collected, stored and processed, a trend that will only continue as increasing numbers of devices are connected to the internet. Most commercial data storage and processing now takes place within huge datacentres run by specialist providers, rather than on individual machines and company servers; the individual elements of this system are obscured to end users within the 'cloud'. One of the technologies that has been instrumental in making this happen is virtual machines.

Normally, a virtual machine (VM) runs just like a real computer, with its own virtual operating system – just as your desktop computer might run Windows. However, a single real machine can run many VMs concurrently. VMs are general purpose, able to handle a wide range of jobs from different types of user, and capable of being moved across real machines within datacentres in response to overall user demand. The University's Computer Laboratory started research on virtualisation in 1999, and the Xen virtual machine monitor that resulted now provides the basis for much of the present-day cloud.

Although VMs have driven the development of the cloud (and greatly reduced energy consumption), their inherent flexibility can come at a cost if their virtual operating systems are the generic Linux or Windows systems. These operating systems are large and complex, they have significant memory footprints, and they take time to start up each time they are required. Security is also an issue, because of their relatively large 'attack surface'.

Given that many VMs are actually used to undertake a single function, (e.g. acting as a company database), recent research has shifted to minimising complexity and improving security by taking advantage of the narrow functionality. And this is where unikernels come in.

Researchers at the Computer Laboratory started restructuring VMs into flexible modular components in 2009, as part of the RCUK-funded [MirageOS project](#). These specialised modules – or [unikernels](#) - are in effect the opposite of generic VMs. Each one is designed to undertake a single task; they are small, simple and quick, using just enough code to enable the relevant application or process to run (about 4% of a traditional operating system according to one [estimate](#)).

The small size of unikernels also lends considerable security advantages, as they present a much smaller 'surface' to malicious attack, and also

enable companies to separate out different data processing tasks in order to limit the effects of any security breach that does occur. Given that resource use within the cloud is metered and charged, they also provide considerable cost savings to end users.

By the end of last year, the unikernel technology arising from MirageOS was sufficiently advanced that the team, led by Dr. Anil Madhavapeddy, decided to found a start-up company. The company, [Unikernel Systems](#), was recently acquired by San Francisco-based Docker Inc. to accelerate the development and broad adoption of the technology, now envisaged as a critical element in the future of the Internet of Things.

"This brings together one of the most significant developments in operating systems technology of recent years, with one of the most dynamic startups that has already revolutionised the way we use cloud computing. This link-up will truly allow us all to "rethink cloud infrastructure", said Balraj Singh, co-founder and CEO of Unikernel Systems.

"This acquisition shows that the Computer Laboratory continues to produce innovations that find their way into mainstream developments. It also shows the power of open source development to have impact and to be commercially successful", said Professor Andy Hopper, Head of the University of Cambridge Computer Laboratory.

Provided by University of Cambridge

Citation: Making operating systems safer and faster with 'unikernels' (2016, January 28) retrieved 27 April 2024 from <https://phys.org/news/2016-01-safer-faster-unikernels.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is

provided for information purposes only.