Bring your own

How hypervisors help integrate portable devices into the office environment. By **David Kleidermacher**

Increasingly, people are using smartphones and tablets for more than business calls – video conferencing, email, document editing, storage and oral presentations are just a few popular applications. This movement towards portable devices is a direct result of the trend towards enterprise mobility, with distributed workforces and portable workspaces.

Security conscious multinational companies prefer to issue approved devices and often explicitly disallow use of corporate phones for personal use and personal phones for corporate use. Furthermore, IT departments are increasingly using enterprise management tools to control mobile devices.

Unfortunately, users dislike these policies almost universally: they force the employee to carry smartphones for company use and for personal use. If permitted to use their corporate phone for personal activities, users often lament lack of privacy and device choice.

The solution to this dilemma is to 'Bring Your Own' smartphone to the office: allowing employees to choose their favourite device and to use it without privacy concerns whilst enabling the same device to be used for work activities, with enterprise usage fully managed by corporate IT. The independence of the personal and enterprise environments has led some to describe these devices as dual persona.

One obvious requirement of a dual persona device is to ensure that cost and features (such as connectivity, graphics and battery life) are not significantly impacted relative to a traditional consumer platform.

Four approaches to dual persona have been commercialised in one form or another:

- Dual boot
- Webtop
- Type 2 hypervisor
- Type 1 hypervisor

• Dual boot

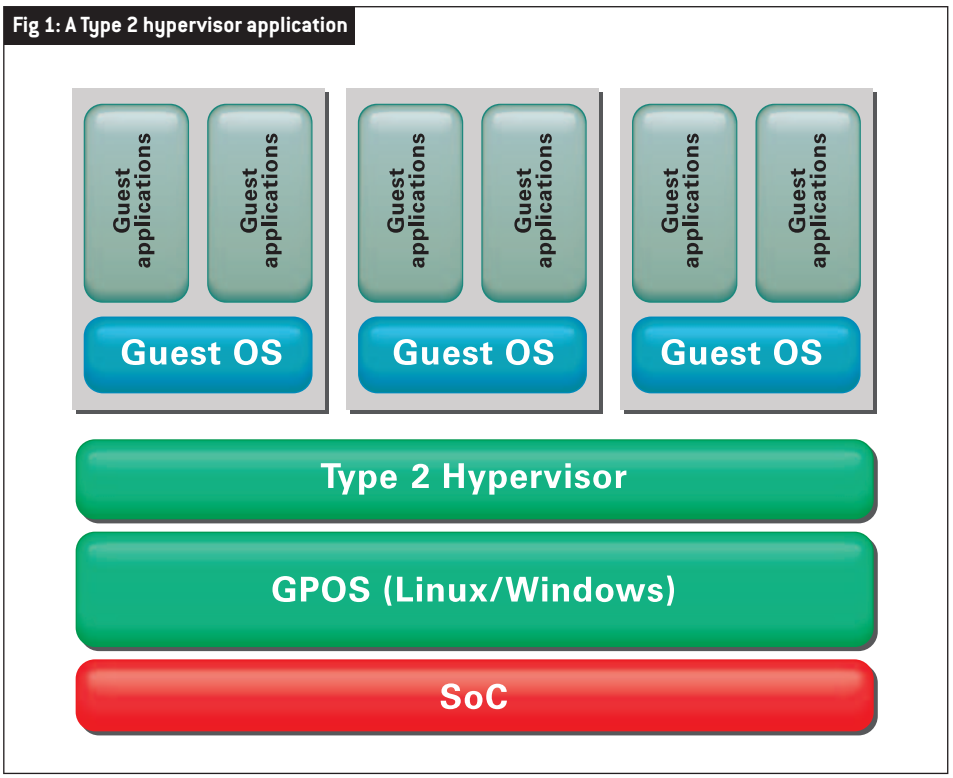
The dual boot concept has been attempted on a handful of laptops and netbooks over the past few years. One example is Splashtop (www.splashtop.com). In a dual boot scenario, a secondary operating system (OS), typically a scaled down Linux, can be launched in lieu of the main platform OS. The scaled down system is typically used for web browsing, the primary goal being to enable the user to browse within a handful of seconds from cold boot. The secondary OS resides in separate storage and never runs at the same time as the primary OS. In some cases, the lightweight environment executes on a secondary microprocessor (for example, an ARM SoC independent of the netbook's main Intel processor).

The secondary OS has good isolation from a security perspective, which both enterprise and consumer appreciate; however, the inconvenience of rebooting and the inability to switch seamlessly between personas has severely limited adoption. Furthermore, because the consumer persona is incapable of much more than simple browsing, it fails to meet the requirement of providing a complete functional replacement of the consumer's desired environment.

• Webtop

The webtop concept also provides a limited browsing environment, independent from the primary user environment. However, instead of dual boot, the webtop runs as an application on top of the primary OS.

Fig 1: A Type 2 hypervisor application



One example is Motorola's Atrix 4G smartphone, whose primary consumer persona is as a fully equipped Android phone. The enterprise persona (or webtop) is a desktop flavour Firefox browser launched when the Atrix is connected to an optional dock with keyboard, mouse and screen.

Because the enterprise persona is simply an application, it suffers from poor isolation from the consumer persona. Practically every smartphone ever built has been rooted. Rooting is the process by which hackers take advantage of some platform vulnerability, such as a kernel flaw, to illicitly obtain superuser privilege and then use this privilege to 'customise' the device. In other words, an Android root file system – even the kernel itself – can be changed or replaced completely.

From a security perspective, IT security administrators must assume the consumer persona has been commandeered. Protecting the enterprise requires the consumer persona and its potentially malicious software are strongly isolated from the enterprise persona. Similarly, users want assurance that the enterprise cannot observe or access anything on the consumer persona. The webtop approach does not meet this requirement.

Furthermore, the webtop's limited enterprise persona – little more than a web browser – again fails to reach functional equivalence to a full featured platform. While the Atrix does permit the enterprise persona to be connected to a remote desktop, the disconnected user – for instance, on an airplane – is unable to work, defeating the purpose of enterprise mobility.

• Type 2 hypervisor

Type 2 hypervisors are similar to webtops in that the secondary persona runs as an application on top of the primary OS. However, instead of hosting only a browser, the secondary persona is a fully fledged guest OS running within a virtual machine created by the hypervisor application (see Fig 1). The hypervisor uses the primary operating system to handle I/O and this virtualisation approach meets the requirement of providing complete functional environments for both personas.

However, the Type 2 model fails to provide strong isolation. Rooting the primary OS enables the commandeering, data stealing or even destruction of the secondary persona. In addition, numerous hypervisor vulnerabilities have been discovered, allowing information 'escapes' between personas.

Fig 2: A microkernel based Type 1 hypervisor

• Type 1 hypervisor

Type 1 hypervisors also provide functional completeness of the dual personas. However, because the hypervisor runs on the 'bare metal', persona isolation cannot be violated by weaknesses in the persona OSs. Thus, a Type 1 hypervisor represents the best approach from both a functionality and security perspective. However, the hypervisor vulnerability threat still exists, and not all Type 1 hypervisors are designed to meet high levels of security.

One particular variant, the microkernel based Type 1 hypervisor, is designed specifically to meet the demanding security requirements of high value enterprises. For example, Green Hills Software's INTEGRITY Multivisor provides strong persona isolation via the INTEGRITY microkernel – the only technology certified to EAL 6+, deemed appropriate for 'management of classified and other high valued information, whose confidentiality, integrity or releasability must be protected', even in the 'presence of both sophisticated threat agents' where the 'likelihood of an attempted compromise is high'.

In addition to isolated virtual machines, the microkernel provides a native, open standard POSIX API for the deployment of lightweight security critical processes, such as device authentication, that cannot be entrusted to a general purpose guest. The Multivisor architecture is shown in Fig 2.

The remaining question is whether virtualised personas can be deployed practically. Historically, mobile device hypervisors have employed paravirtualisation – customised guest OSs – to account for the lack of mobile processor hardware virtualisation assistance; something that has been available in desktops and servers for years.

Paravirtualisation has proven prohibitively expensive and slow to market. The great news is that many current generation smartphones and tablets support ARM's TrustZone technology that provides a form of high speed virtualisation. In addition, ARM's Virtualisation Extensions, a complete hypervisor mode for mobile ARM applications processors and due in apps processors in 2012, will further improve the platform for hypervisors.

In other words, the future of 'Bring Your Own' is bright.

Author profile:
David Kleidermacher is Green Hills Software's chief technology officer.