InZero Technologies

Patented SmartHyp™ Bare-metal Type-1 Mobile Virtualization

Solving the Power
& Performance Problems

1. IN A NUTSHELL

In the last several years, mobile device architecture has increasingly provided bare-metal (Type-1) hypervisor enablement. However, mobile hypervisors created to date continue to experience the primary shortcomings – power drain and poor performance – that have made mobile hypervisor use unappealing, despite the strong security offered in the Type-1 bare-metal hypervisor. These issues have plagued attempts to develop Type-1 mobile hypervisors for over a decade.

Therefore, we specifically designed the InZero Type-1 mobile hypervisor to overcome these issues, through a novel approach implementing two key technical innovations.

First, we control VM execution, so that only the active VM in use consumes the full resources of a typical VM, while we control resource use of other VMs to minimize resource constraints. In addition, InZero Virtualization also provides direct hardware interface driver access, eliminating performance issues by eliminating resource-consuming paravirtualization.

Furthermore, for added security, InZero's Virtualization also includes the new InZero "TrustWall", a hardware-enforced firewall (executing in parallel in its own dedicated VM) that, in the event of organization network infection (for any reason), prevents exfiltration of network data – in other words, it renders a successful malware attack on the company intranet futile for the hacker. TrustWall is optional.

In either implementation, with or without TrustWall, InZero Virtualization provides for power consumption and performance akin to typical mobile device use as if operating without hypervisor.

2. DESPITE A DECADE OF DEVELOPMENT, POWER AND PERFORMANCE PROBLEMS CONTINUE

In 2006, VMware tasked its internal developers with creating a Type 1 mobile hypervisor. But in 2008, VMware changed course and acquired Trango – creators of a supposedly effective existing Type-1 hypervisor – and in late 2008, VMware announced the impending introduction of the Trango hypervisor:

"VMware acquires Trango, debuts mobile hypervisor" (NetworkWorld, November 2008)

However, two years later, the strategic winds of VMware shifted again, this time eschewing the Type 1 hypervisor for the less-secure Type-2 –

> ***"VMware rethinks it plans for a mobile hypervisor"***
>
> *"In a surprising about-face VMware has stepped back from its previously announced plans to release a type I hypervisor in support of its bid to address the mobile hypervisor market and VMware has set its sights lower redefining MVP as a type II hypervisor …. The fundamental difference between a type I and a type II hypervisor is that the former runs on bare metal, between the hardware and the operating system; where a type II hypervisor runs on top of an OS. That **difference is crucial**." (TVP Strategy, 2010, emphasis added)*

The next two years did not see the industry introduce a universally welcomed Type-1 hypervisor, despite the growing realization that mobile devices need to address data separation between sensitive network data and everything else:

100 Carpenter Drive, Sterling, VA 20164

> ***"Mobile Hypervisors Will Spur BYOD Adoption, but not this year"***
>
> *"Not quite ready for prime time, but well beyond the point of speculation, mobile hypervisors are set to start reshaping the way that businesses and consumers will view the mobile devices."*
> (TVP Strategy, 2012)

But the problems of the mobile hypervisor — power and performance — persisted. In "The Study and Evaluation of ARM-Based Mobile Virtualization" (Sage Journals, October 2014), the authors concluded:

> *"Undisputedly, as mobile computing advances, it brings several tough challenges, described as follows.*
>
> *(1) Security. Mobile device, as a kind of intimate personal portable equipment, contains lots of user's sensitive data.*
>
> *(2) Performance Wasting. It seems that these vendors participated in a hardware competition which led to a serious performance wasting. How to make better use of hardware resources is a new challenge.*
>
> *(3) Power Consumption. Power is always the bottleneck of mobile devices*."

The authors urged that hypervisor hardware architecture needed "small code size," "strict system-wide security", "minimal impact on system resources", and needed to "be suitable for ARM architecture".

The same fundamental challenges were recognized in "A Survey of Mobile Device Virtualization: Taxonomy and State-of-the-Art" (ResearchGate July 2016):

> *"Mobile devices are resource constrained and virtualization leads to performance overhead in any case…. Mobile virtualization solutions need to maintain real-time capability of mobile devices while hosting multiple OSs on resource constrained hardware." (Emphasis added.)*

3. THE WORKPLACE IS MORE READY THAN EVER

According to Global Information, Inc.'s recent study, "Global Mobile Virtualization Market Insights, Opportunity Analysis, Market Shares and Forecast, 2016 – 2022":

- *"The increasing need to isolate personal and work data is one of the factors fueling the growth of the mobile virtualization market".*
- *The global mobile virtualization market is estimated to grow from USD 2.16 billion in 2016 to USD 5.68 billion by 2021, at a CAGR of 21.3% during the forecast period. Major factors driving the mobile virtualization market are increasing need to isolate personal and work data, high level of security in mobile applications, and flourishing mobile industry.*
- *"Hypervisor segment to account for the largest market share during the forecast period"*
- *Based on technology, the hypervisor segment of the global mobile virtualization market is estimated to account for the largest market share during the forecast period.*

4. . . . AND INZERO IS READY FOR THE MARKETPLACE

InZero's initial Type-1 Virtualization is based on the popular Xen hypervisor, and is ready for demonstration and adoption to specific mobile device architecture.

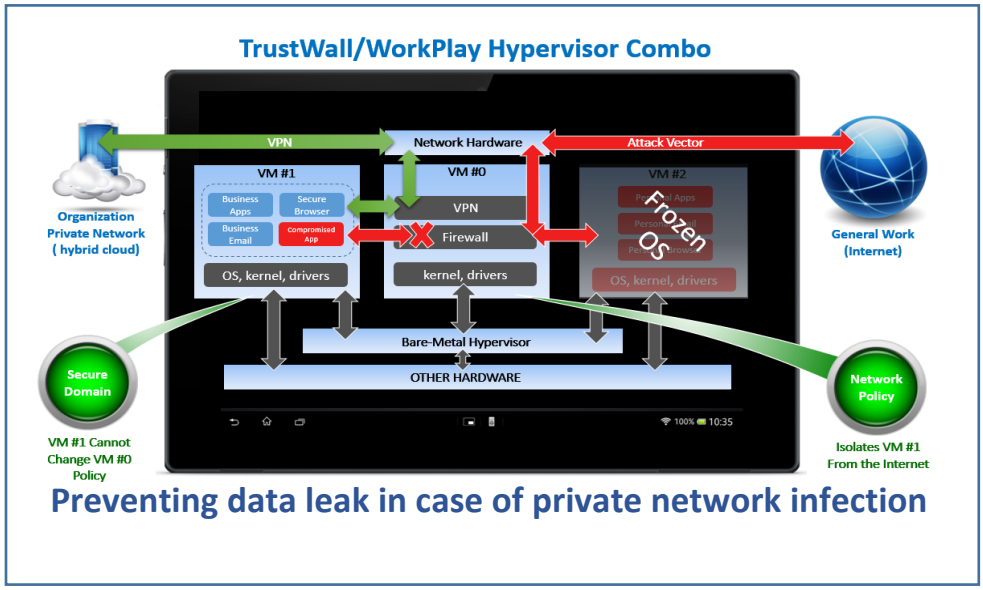
In its most basic expected implementation, one VM is dedicated to the organizational network while the second VM freely accesses the internet (or as desired, implements a different level of security than VM No. 1.)

With TrustWall, three VMs are easily created – two functioning VMs and one mini-VM in-between the operating VMs, so to speak, to create TrustWall employing ARM TrustZone Secure World.

The resulting combination of the InZero Virtualization and TrustWall:

- Provides Type-1 bare-metal security
- Eliminates the excessive power drain of hypervisors executing in parallel
- Eliminates the unsatisfactory performance caused by the resource constraints of paravirtualization
- Protects against intranet exfiltration in case of network infection regardless of nature or cause of infection, and prevents cross-contamination between VMs

We have successfully tested InZero Virtualization, please feel free to contact us for a demonstration and details.



InZero Technologies

100 Carpenter Drive, Sterling, VA 20164

www.inzerosystems.com