

## Virtsec: Virtualization Security

By David Kleidermacher

Aided by the migration of hardware virtualization assistance into embedded processors, hypervisor technology is now beginning to sprout up in real time telecommunications, mobile devices and other electronics. However, embedded systems have different requirements from data centres and a highly secure virtualization environment enables some compelling applications that are suited for embedded and portable gear.

### Virtualization insecurity

VMware products were recently evaluated to Common Criteria EAL 4, the same security level that has been previously reached by Windows and Linux. Table 1 provides a brief summary of the security assurance levels specified by Common Criteria (more formally known as ISO/IEC 15408, an international standard for evaluating security).

|       |   |
|-------|---|
| EAL 1 | Functionally tested                         |
| EAL 2 | Structurally tested                         |
| EAL 3 | Methodically tested and checked             |
| EAL 4 | Methodically designed, tested, and reviewed |
| EAL 5 | Semiformally designed and tested            |
| EAL 6 | Semiformally verified design and tested     |
| EAL 7 | Formally verified design and tested         |

*Table 1: Common Criteria Security Levels*

According to Common Criteria, EAL 4 is 'the highest level at which it is likely to be economically feasible to retrofit an existing product line [1]'. The security specifications of EAL 4 products admit that they are not appropriate when 'protection is required against determined attempts by hostile and well funded attackers [2]'.

Therefore, it should come as no surprise that a number of studies of virtualization security and successful subversions of hypervisors [3] and [4] have been published. The risk of an 'escape' from the virtual machine layer, exposing all the guests is very real. As one analyst has said 'virtualization is essentially a new operating system ... and it enables an intimate interaction between underlying hardware and the environment. The potential for messing things up is significant [5]'.

There is more to security than using the words 'secure' or 'trusted' in product names. Unfortunately, the public is often misled by such marketing and users have become accustomed to the fail first, patch later mentality of insecure software. Thus, much of the world's critical

infrastructure, financial networks, medical information systems, telecommunications gear and portable mobile devices run insecure operating systems and hypervisors that leave them open to compromise.

### Secure virtualization

Hypervisor architectures typically employ a monolithic architecture, as shown in Figure 1. Similar to monolithic operating systems, the monolithic hypervisor requires a large body of operating software, including device drivers and middleware, to support the execution of one or more guest environments. In addition, the monolithic architecture often uses a single virtualization component (itself a complicated piece of software) to support multiple guest environments. Thus, a single flaw in the hypervisor may result in a compromise of the fundamental guest environment separation intended by virtualization in the first place.

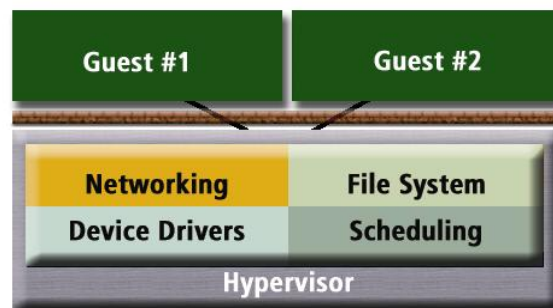


Figure 1: Monolithic Hypervisor architecture

An alternative, but similarly insecure, approach uses a trimmed down hypervisor that runs in the microprocessor's privileged mode but employs a special guest operating system to handle the I/O control and services for the other guests (Figure 2). Thus, a complex, monolithic body of software must still be relied upon for system security.

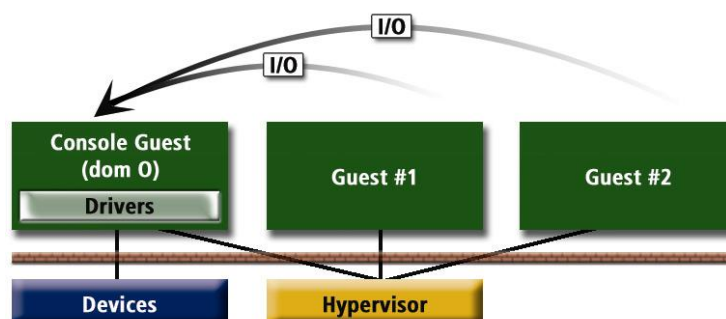


Figure 2: dom0 monolithic architecture

A different architecture is required to provide robust separation between guest environments. Figure 3 shows Green Hills Software's virtualization architecture.

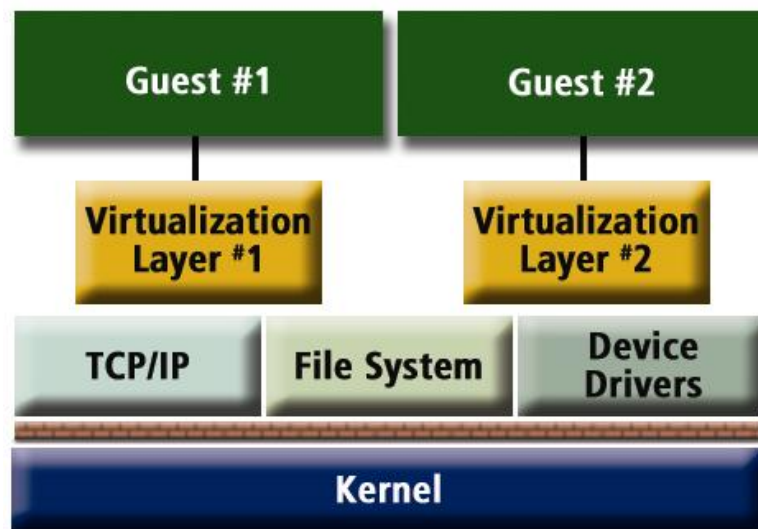


Figure 3: Microkernel based hypervisor architecture

This architecture places the virtualization complexity and related I/O drivers and middleware into user mode applications, outside the trusted computing base which contains only the secure microkernel: Green Hills Software's INTEGRITY.

INTEGRITY provides low level hardware support, resource partitioning, and scheduling for the virtual environments. Furthermore, a separate instance of the virtualization infrastructure is used for each guest environment, precluding cross VM escapes.

INTEGRITY is the first operating system or virtualization technology certified to a high assurance level under Common Criteria [6]. Designed for EAL 7, the highest security level, INTEGRITY meets what the US National Security Agency deems required for 'high robustness' – protection of national secrets in the face of attack by highly determined and resourceful enemies [7].

This operating system is currently being used in NSA approved cryptographic communications devices, avionics systems that control passenger and military jets, life critical medical systems, secure financial transaction systems, and a wide variety of other safety and security critical systems.

INTEGRITY provides a full-featured application programming interface (API) and software development kit, enabling secure software that cannot be trusted to run on a guest. Thus, critical applications and data such as firewalls, hard real-time components, digital identity and financial transaction applications, and cryptographic subsystems can be deployed alongside, but securely separated from, the general purpose environments such as Windows and Linux. The combination of virtualized and native applications on a single processor provides a compelling cost and power

efficient operating environment (Figure 4), ideal for embedded electronics and portable devices. This hybrid model also takes advantage of multicore processors by enabling concurrent execution of native and virtualized subsystems.

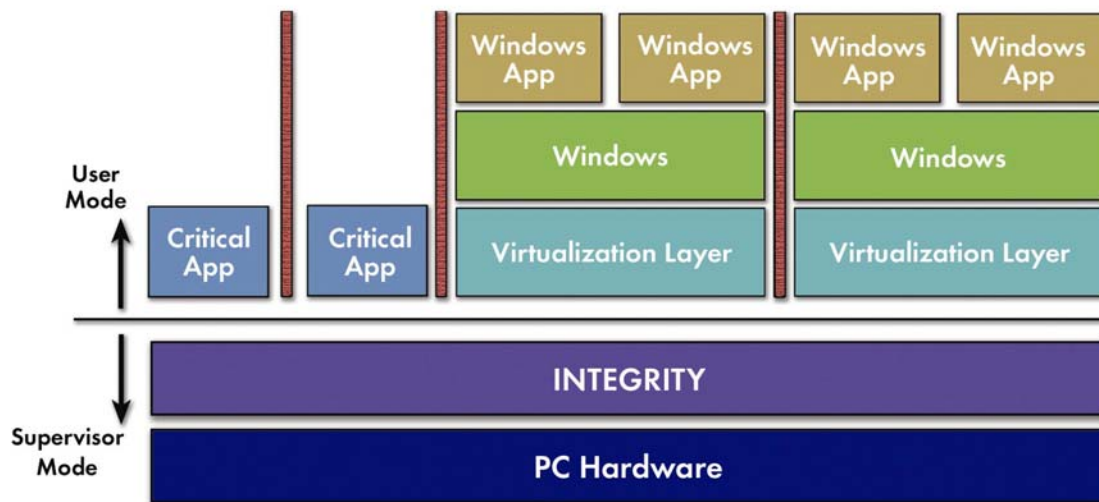


Figure 4: Virtualized environments alongside native applications

Among its many stringent requirements, the high assurance security evaluation requires formal methods to mathematically prove the security policies that ensure separation of the guest environment from other guest environments, from security-critical applications, and from the trusted kernel itself.

The flexibility afforded by virtualization has proven powerful in the data center and promises even more varied and compelling advantages throughout the electronics world. However, the proper virtualization architecture can drastically improve security without sacrificing the utility of legacy software. Green Hills Software's INTEGRITY, with virtualization technology, is appropriate for electronic products that demand a high level of security, reliability, and functionality.

## References

- 1: *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1*; Section 6.2.4
- 2: *Controlled Access Protection Profile*;  
[www.radium.ncsc.mil/tpep/library/protection\\_profiles/CAPP-1.d.pdf](http://www.radium.ncsc.mil/tpep/library/protection_profiles/CAPP-1.d.pdf)
- 3: Samuel King, et al., "SubVirt: Implementing malware with virtual machines", <http://www.eecs.umich.edu/virtual/papers/king06.pdf>, 2006
- 4: Tavis Ormandy, "An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments", <http://tavis0.decsystem.org/virtsec.pdf>, 2007

5: Rich Ptak quoted by Denise Dubie, *"Security concerns cloud virtualization deployments"*,

<http://www.networkworld.com/news/2007/112107-security-virtualization.html>, *Network World*, November 21, 2007

6: *INTEGRITY-178B - NIAP validated product*;

<http://www.niap-ccevs.org/cc-scheme/st/vid10119/>

7: *Protection Profiles Frequently Asked Questions*;

<http://www.niap-ccevs.org/cc-scheme/faqs/pp-faqs.cfm#robustness>

**Author profile:**

David Kleidermacher is Green Hills Software's chief technology officer.  
davek@ghs.com, [www.ghs.com](http://www.ghs.com)