Kaspersky®
Secure Hypervisor

Kaspersky Secure Hypervisor: Zero tolerance to insecurity

The goal of the solution is to make it possible to run multiple virtual machines (guest operating systems) on a single physical machine, distributing physical resources among guest systems.

Introduction

When it comes to the adoption and success of embedded systems, security is a key factor in a world where professional hackers and APTs are the harsh everyday reality. Threats vary, from attacks on exposed interfaces to the undocumented or aggressive behavior of peripheral equipment (e.g. PCI, USB). After a successful attack, an intruder can go further, for example, by exploiting operating system vulnerabilities, potentially threatening critical processes. Despite the vulnerabilities and large attack surface of general-purpose systems, vendors prefer popular platforms because of the widespread availability of software.

Virtualization technology presents an opportunity to harden system security, while retaining the ability to reuse an existing code base.

Purpose

Kaspersky Secure Hypervisor is a type-2 hypervisor that runs on the KasperskyOS microkernel and utilizes its security capabilities, turning KasperskyOS into a hypervisor solution.

The goal of the solution is to make it possible to run multiple virtual machines (guest operating systems) on a single physical machine, distributing physical resources among guest systems. Normally, virtualization is supported by modern CPU capabilities that give guest operating systems a performance close to that of a dedicated physical machine.

The main benefit of a virtualization solution is the separation of potentially untrusted guest operating systems from each other and from critical services collocated on the same physical machine, reducing the attack surface and minimizing the possible impact of exploited vulnerabilities. The hypervisor is protected from guest OS actions in such a way that malicious activities by a guest system cannot damage the critical services or the hypervisor itself.

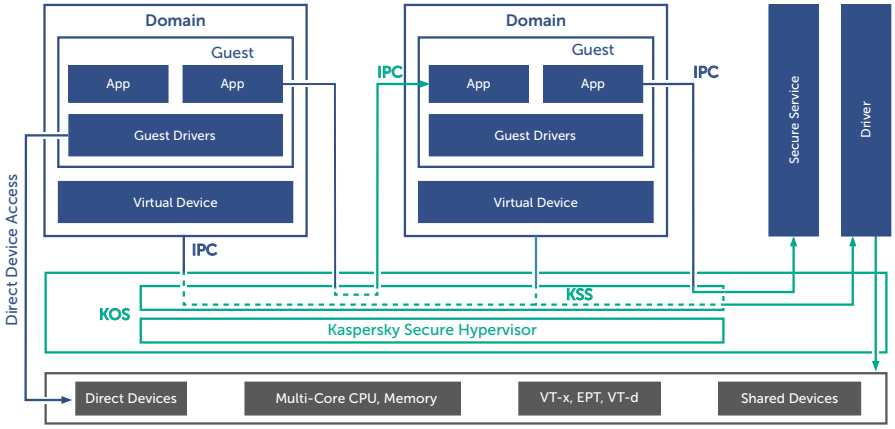
Features

Kaspersky Secure Hypervisor contains two software components: one running in a privileged kernel mode, and the other running in a user mode. The privileged kernel component is responsible for the management of resources (e.g. memory, CPU) and provides access to I/O devices. User mode components of Kaspersky Secure Hypervisor include common host user-mode device drivers and a special guest driver, called KL secdev, that provides communication channels between domains or between a domain and the hypervisor itself.

One of the security benefits of device emulation is that the hypervisor can intercept all the transactions between a guest OS and the device and implement additional security measures that a guest OS cannot bypass

Kaspersky Secure Hypervisor uses virtualization support for hardware devices to create virtual environments (domains) that share a common CPU and memory. If present, hardware virtualization features can be used to pass through PCI devices (such as a video adapter, network adapter, hard disk controller, USB) to guest OSs. This technique improves the performance of these devices but makes sharing impossible. See the list of emulated and passed-through devices below.

If sharing of devices is required, we use a user-space device emulation technique. The idea is to run a KasperskyOS user-space driver with direct access to a device that needs to be shared. The driver implements device emulation, i.e. it provides an interface for guest OSs that can be used to access a device, without guest OSs knowing that the device is virtual. One of the security benefits of device emulation is that the hypervisor can intercept all the transactions between a guest OS and the device (e.g. network card, SATA controller) and implement additional security measures (e.g. traffic filtering, encryption) that a guest OS cannot bypass. Device emulation can also be used when hardware virtualization features are not available.



In-Vehicle Infotainment

In this architecture, two domains are used: one for mission-critical software (vehicle control, network software) and another for non-critical infotainment software (media, connectivity, voice features, user interface). Separate virtual environments ensure the stability of mission-critical software whatever action the user takes. With the device emulation technique, shared hardware (such as network card, GSM or Wi-Fi modules) can be used by domains, reducing the hardware costs. This architecture also makes it possible to keep the infotainment software up to date without affecting critical components during software updates.

Industrial Security Systems

In this architecture, two or more domains are used to separate industrial software, communication software, databases, and user interfaces.

Mobile Devices

A hypervisor solution can create separate domains or profiles for (1) corporate data and critical applications (e.g. broadband software stack, VPN, security services, storage for certificates and credit cards) and (2) personal data. This approach helps to separate confidential business data, communications and private information from each other.

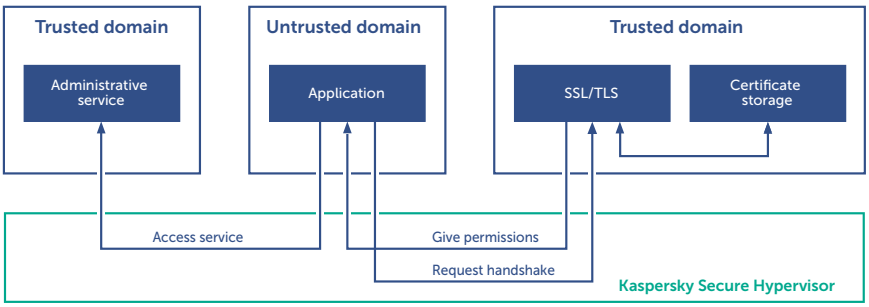
Implementation

We see Kaspersky Secure Hypervisor as a trusted framework for:

- IoT
- Automobiles
- Healthcare
- Industrial automation
- Point-of-sale terminals
- Thin clients and VDIs
- Corporate tablets and smartphones

Secure Storage for Certificates and Keys

In this architecture, certificate storage and encryption services are kept in a separate trusted domain. Guest OS applications run in another domain, and get access to encryption services via Kaspersky Secure Hypervisor communication channels. With proper authentication, the trusted components can give additional privileged permissions to guest OS applications (e.g. permissions to administrative services). Even if guest OS applications have been hacked, they cannot get access to keys or escalate their privilege due to the security policy enforcement and domain separation guaranteed by the hypervisor.

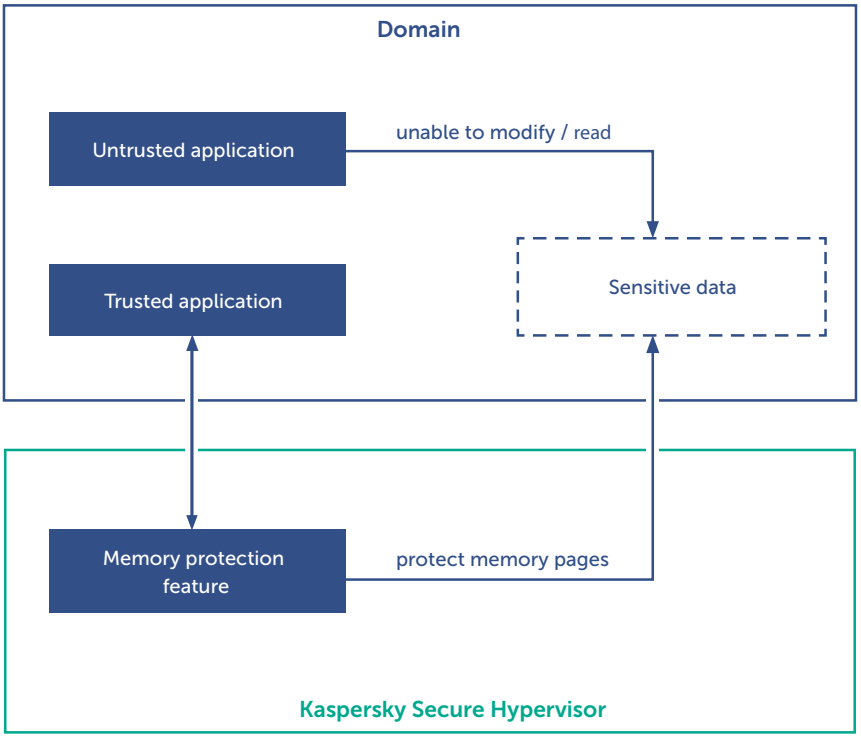


Network Analysis and Filtering

In this architecture, all network communications between guest OS applications and the external world are filtered transparently (i.e. with no modification to guest OS applications and with guest OS applications unaware of filtering). If needed, traffic inspection can be implemented, remaining invisible to potential attacks from guest OS applications. Even if guest OS applications have been compromised, they cannot bypass filtering and send data to a remote party.

Protection of Sensitive Guest OS Data

Kaspersky Secure Hypervisor is capable of protecting a guest OS's sensitive data from modifications or unauthorized access via a memory protection mechanism. Memory protection is achieved by setting appropriate permissions to guest physical pages. In a typical scenario, a guest OS calls Kaspersky Secure Hypervisor to protect the guest OS's sensitive data before running an untrusted application. Examples of protectable data include guest OS kernel code, guest security services, and configurations.



Technical requirements

- **Host OS.** Kaspersky Secure Hypervisor is a type-2 hypervisor provided with KasperskyOS as a host system.
- **Platforms.** Intel x86 or x64 with support for VT-x and (optionally) VT-d technology. Support for ARM is in progress.
- **Guest OSs.** Unmodified Linux-based distributions such as Ubuntu and CentOS can be used as guest operating systems, on both x86 and x64 variants. Support for other guest environments (primarily, Windows) is in progress.
- **Emulated devices.** x86 legacy (PIC, PIT), PCI bus, NE2000, IDE/ SATA controller, UART (COM port).
- **Tested pass-through devices.** USB controller, SATA controller, PCI Ethernet, Radeon/nVIDIA video cards, legacy IDE controller.

Patents

The technologies that form the basis of KasperskyOS and Kaspersky Security System are covered by a set of patents:

US 7386885 B1, US 7730535 B1,
US 8370918 B1, EP 2575318 A1,
US 8522008 B2, US 20130333018 A1,
US 8381282 B1, EP 2575317 A1,
US 8370922 B1, EP 2575319 A1,
US 9015797 B1, DE 202014104595 U1

Advantages

1. **Proprietary solution.**
   Kaspersky Secure Hypervisor is a proprietary solution fully supported by Kaspersky Lab. The development process is based on best practices with systematic testing and verification.
2. **Strong isolation and mediated communications.**
   Kaspersky Secure Hypervisor utilizes KasperskyOS features, providing the means to run multiple guest operating systems and KasperskyOS native applications on a single machine. Isolation between domains is guaranteed by the kernel component of Kaspersky Secure Hypervisor. All communications between domains and between a domain and the kernel are mediated by Kaspersky Security System according to a predefined security policy. Even if an attacker performs a virtual machine escape, further actions are limited by the security policy.
3. **Flexible access control.**
   Kaspersky Security System is grounded on an attribute-based model and supports a wide range of policies (e.g. object capabilities, flow control, Type Enforcement and multilevel security). Its flexible, extendable nature makes it possible to develop custom domain-specific policies relevant to an application area.
4. **Resource management for guest OSs.**
   Kaspersky Secure Hypervisor restricts the amount of resources (such as memory or physical device access) available to guest systems to protect the whole environment from possible resource exhaustion attacks coming from guest OSs. Potentially dangerous external devices can be restricted, so that erroneous or malicious hardware is unable to access the memory of guest operating systems or the hypervisor.
5. **Ability to integrate with secure boot system.**
   Kaspersky Secure Hypervisor includes features to guarantee the integrity of the hypervisor and guest OSs.
6. **Small trusted computing base.**
   When used with KasperskyOS as a host OS, Kaspersky Secure Hypervisor benefits from the KasperskyOS microkernel design, providing a small verifiable trusted computing base (TCB)*. All device drivers are run in a host user mode, further reducing the risk of a hypervisor being damaged or hijacked.

---

* Trusted computing base (TCB) is the set of all components (hardware, firmware and software) critical to overall security of a solution. Small TCB facilitates exhaustive testing and verification.

www.kaspersky.com

Find out more at os.kaspersky.com
All about Internet security: www.securelist.com