Title (en)

SECURE VIRTUAL-MACHINE MONITOR

Title (de)

SICHERE VIRTUELLMASCHINEN-ÜBERWACHUNGSVORRICHTUNG

Title (fr)

MONITEUR DE MACHINE VIRTUELLE SECURISE

Publication

EP 1955154 A2 20080813 (EN)

Application

EP 06826781 A 20061025

Priority

- US 2006041851 W 20061025
- US 73047805 P 20051025

Abstract (en)

[origin: WO2007050797A2] Embodiments of the present invention provide secure virtual-machine monitors and secure, base-level operating systems that, in turn, provide secure execution environments for guest operating systems and certain special functions that can interface directly to base-level operating systems. Security is accomplished by employing a small, verifiable component of a secure foundation that executes at highest privilege between the hardware interface and the virtual-machine monitor. The virtual-machine monitor and secure foundation employ virtual-machine-monitor-resident guest-operating-system monitors, memory compartmentalization, and authenticated calls to securely isolate computational entities from one another within the computer system.

IPC 8 full level

G06F 9/455 (2006.01)

CPC (source: EP)

G06F 9/45558 (2013.01); **G06F 21/53** (2013.01); G06F 2009/45566 (2013.01); G06F 2009/45583 (2013.01); G06F 2009/45587 (2013.01)

Citation (search report)

See references of WO 2007050797A2

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

Designated extension state (EPC)

AL BA HR MK RS

DOCDB simple family (publication)

WO 2007050797 A2 20070503; **WO 2007050797 A3 20090507**; EP 1955154 A2 20080813; JP 2009514104 A 20090402

DOCDB simple family (application)

US 2006041851 W 20061025; EP 06826781 A 20061025; JP 2008537955 A 20061025