7-Minuten-Pitch

Zertifizierte Betriebssysteme auf Mikrokern-Basis für Hochsicherheitsanwendungen

Thomas Günther, INFODAS GmbH, Köln

Dr. Michael Hohmuth, Kernkonzept GmbH, Dresden

infodas

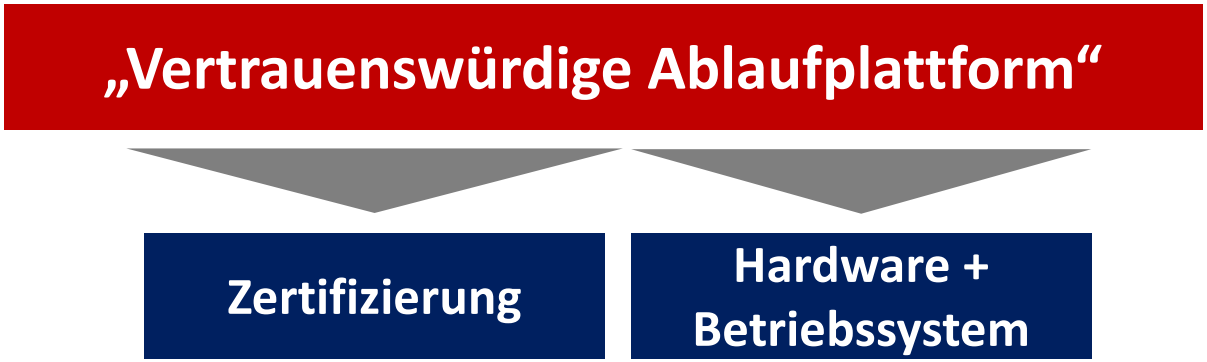
KERNKONZEPT

Hochsicherheitsanwendungen: Anwendungsbeispiele

- Sichere, bidirektionale Netzübergänge
- Netzwerkdioden
- Firewalls
- Labelling-Dienste
- Elektronische VS-Registraturen
- Virenschutzsysteme, IDS, IPS
- Anwendungen in kritischen Infrastrukturen

Hochsicherheitsanwendungen haben sehr spezielle Anforderungen

- Hohe Anforderungen an
  - Hardware und Kryptographie,
  - Selbstschutz- und Selbsttests,
  - Robustheit gegen physische Angriffe, etc.
- Zusätzliche, herausfordernde Anforderung:

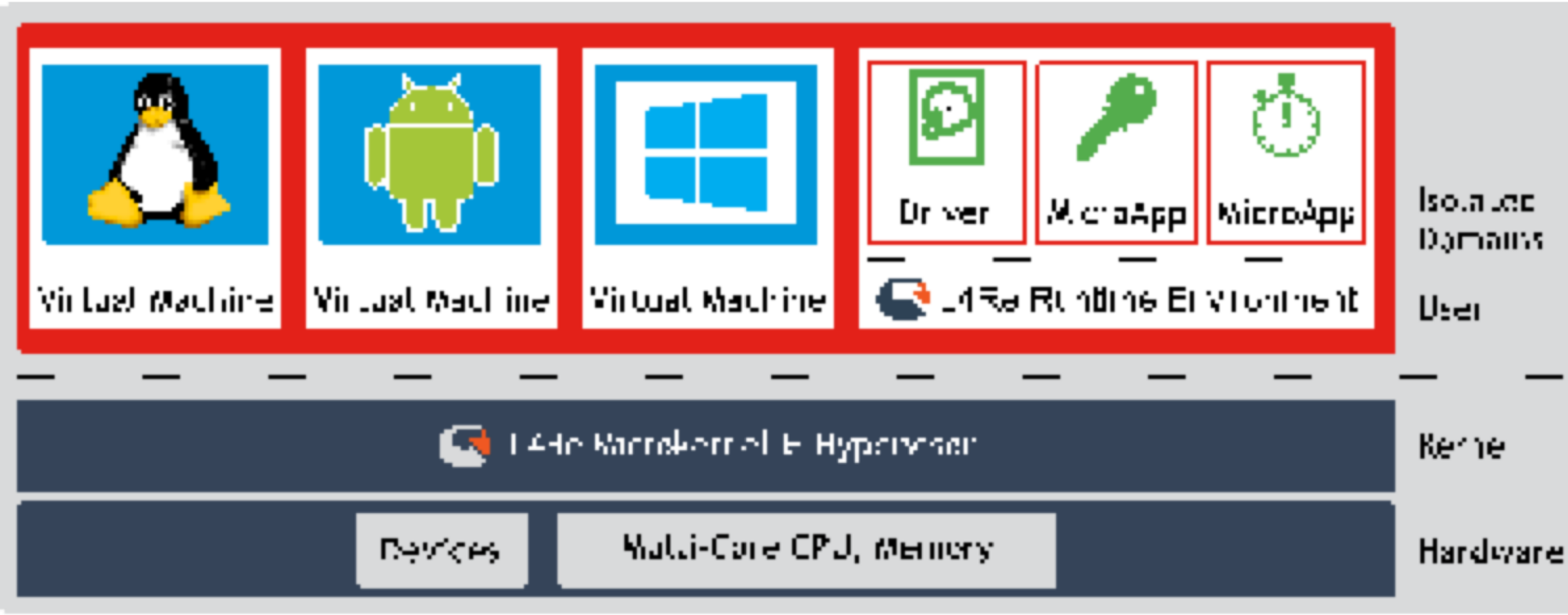


„Vertrauenswürdige Ablaufplattform“ für sicherheitskritische Anwendungen

- Nachweis der sicherheitstechnischen Funktions-weise
- Separierungs- und Isolierungsmechanismen (dienen auch dem Selbstschutz)
- Überwachung der Kommunikation
  - zwischen Prozessen untereinander
  - zwischen Prozessen und Hardware
- Kombination aus Hardware und Betriebssystem bildet die „Vertrauenswürdige Ablaufplattform“

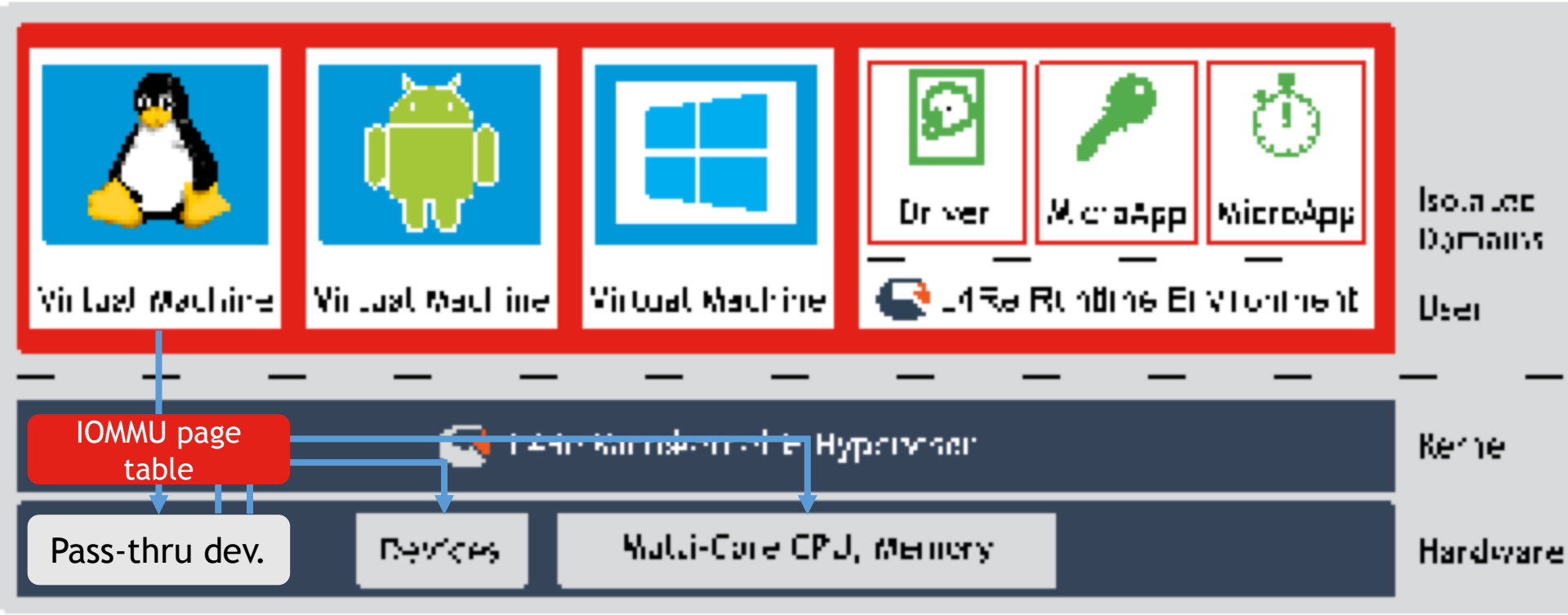
ACHTUNG! Hardware ist üblicherweise nicht vertrauenswürdig!

SDoT MOS: Evaluierbarkeit



- Microkernel garantiert Isolation
- Kleine Trusted Computing Base für Sicherheitsfunktion
- Virtuelle Maschinen mit Standard-Systemsoftware

SDoT MOS: Separierung von Hardware-Komponenten und Peripherie



- Verhinderung unbeschränkter DMA-Zugriffe

SDoT MOS: Sichere, aber flexible Kommunikation

- Anwendungsvielfalt und Flexibilität
  - Kommunikationsverfahren: Virtuelles Netzwerk, Sockets, Shared Memory, Microkernel-IPC
- Herausforderung: Zertifizierbarkeit der Plattform
  - Keine Weitergabe von Zugriffsrechten möglich
  - Kommunikationsmechanismus hat keinen Zugriff auf Anwendungsspeicher
- Lösung in SDoT MOS: Pure Channels
  - Eigenschaft für Kommunikationsmechanismen
  - Separat oder mit Anwendung zertifizierbar
  - „Pure Channel“ Linux-Sockets bereits enthalten

Fazit

- Security Appliances benötigen eine sichere und vertrauenswürde Ablaufplattform
- SDoT MOS erfüllt die Anforderungen an Evaluierbarkeit
- SDoT MOS ist für zukünftige, sicherheits-kritische Anwendungen eine geeignete Basis.

Vielen Dank für Ihre Aufmerksamkeit.

Mehr an unserem Stand…!

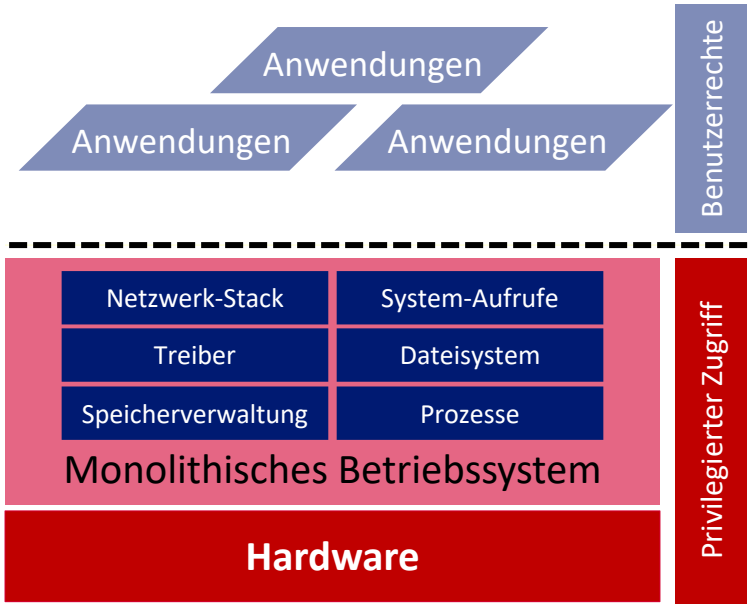
infodas

KERNKONZEPT

Backup

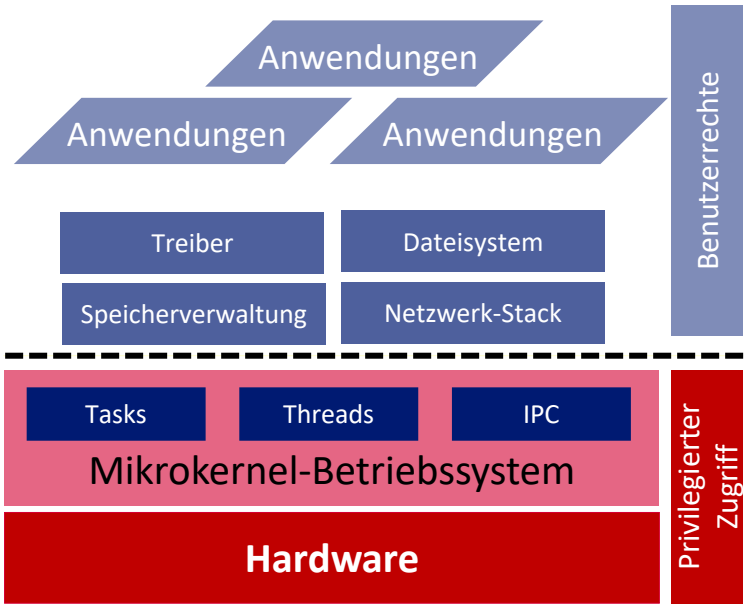
Mikrokern schränkt privilegierten Zugriff auf Hardware stark ein

Monolithisches Betriebssystem



- Treiber, Speicherverwaltung und Dateisystem sind Bestandteil des Betriebssystem und haben vollen Zugriff auf die Hardware
- Nur End-Anwendungen laufen mit eingeschränkten Rechten

Mikrokernel-Betriebssystem



- Nur minimalistischer Betriebssystem-Kern mit vollen Rechten
- Viele Betriebssystem-Dienste haben nur eingeschränkte Benutzerrechte
- Definierte Schnittstellen

Sicherheitstechnische Anforderungen an ein zertifizierungsfähiges Betriebssystem

- Separierung von Prozessen
  - Virtuelle Speicherverwaltung
  - Zugriffsschutz auf Kernobjekte des Betriebssystems
  - Kontrolle der Inter-Prozess- und Inter-Kompartment-Kommunikation
- Separierung von Hardware-Komponenten
  - Kompartments erhalten eingeschränkten Zugriff auf Hw
  - Keinerlei Zugriff auf nicht zugewiesener Hw
- Unterstützung eines sicheren Bootens
  - Nachweis der Korrektheit der geladenen Anwendung
  - Verhinderung der Ausführung von Fremdcode während des Bootprozesses

Evaluierbarkeit durch Mikrokern

- Kleiner Anteil des Betriebssystems läuft im „privilegierten“ Modus des Prozessors
- Reduktion auf das absolute Minimum
- Grundsätzliche Evaluierbarkeit aufgrund der geringen Lines of Code möglich