Plattformsicherheit durch vertrauenswürdige Virtualisierung

Konzept, Anwendung und Architektur am Beispiel OpenTC

Dirk Kuhlmann
Hewlett Packard Laboratories Bristol

© 2006 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice

Kombination von Virtualisierung mit TCG-Technologie

- Perspektive des Vortrags:
  - Hardware- und Systemhersteller
  - *XEN* als Basissystem („L4-inspiriert“, Ergebnisse i.d.R. übertragbar)
  - Client-Architektur: “Trusted Converged Clients”
- Kontext: FP6 Projekt *Open Trusted Computing*
- Ziele:
  - Virtualisierung zur Isolation von Softwarekomponenten
    - Mechanismen zur Reduktion der Trusted Computing Base
    - Kapselung von privilegiertem Code
  - Überprüfbare Integrität, Konfiguration und Policies fuer virtualisierte Komponenten
  - Verantwortungsgerechter Einsatz von TCG-Technologie

hp invent

Motivation

- Status Quo: Betriebssystem ist z.Zt. “Vertrauensanker”
  - Determinante fuer Sicherheit der Hardware-Plattform
- Virtualisierung erlaubt Implementation neuer Kontrollmechanismen
  - Auf VMM Ebene, d.h., unabhaengig vom Betriebssystem
    - => policies niedriger Granularität
- Traditioneller Fokus von VMMs:
  - Performance, breite Funktionalität, Benutzerfreundlichkeit
  - Sicherheitseigenschaften und -architektur eher zweitrangig
- Verbesserung der VMM-Sicherheitsarchitektur
  - *XEN Kontroll-OS* (Dom0) enthält den Grossteil privilegierten Codes
    - Auslagerung von Kontrollfunktionen in generische Services
    - Bessere Vertrauenswürdigkeit der Isolationseigenschaften

hp invent

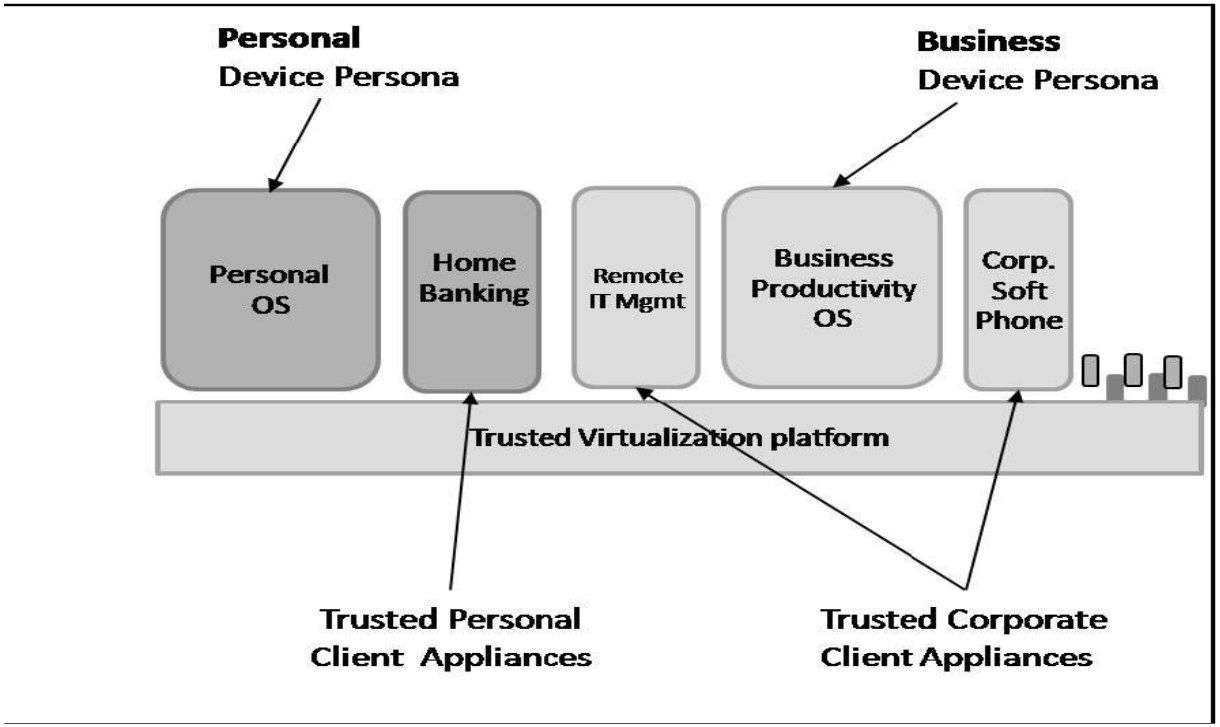
Trusted Virtual Platforms

- Globale Integritätsüberprüfungen:
  - Hypervisor / VMM
  - Device Model (Netzwerk, Grafik)
  - Sicherheitsservices (etwa globale Firewalleinstellungen)
- Lokale Integritätsüberprüfungen:
  - Einzelne VMs und Appliances
- Erlaubt Trennung von VMM und VM-Integritaet und Policies
  - Beispiel: lokaler (VM) und globaler Firewall
- Erfordert Virtualisierung des Trusted Computing Moduls
  - Erweiterung des Integritätsmodells
  - Abhängigkeits-Baum statt linearer Kette
- Zentraler Baustein fuer „Trusted Converged Clients“

hp invent

“Trusted Converged Clients”

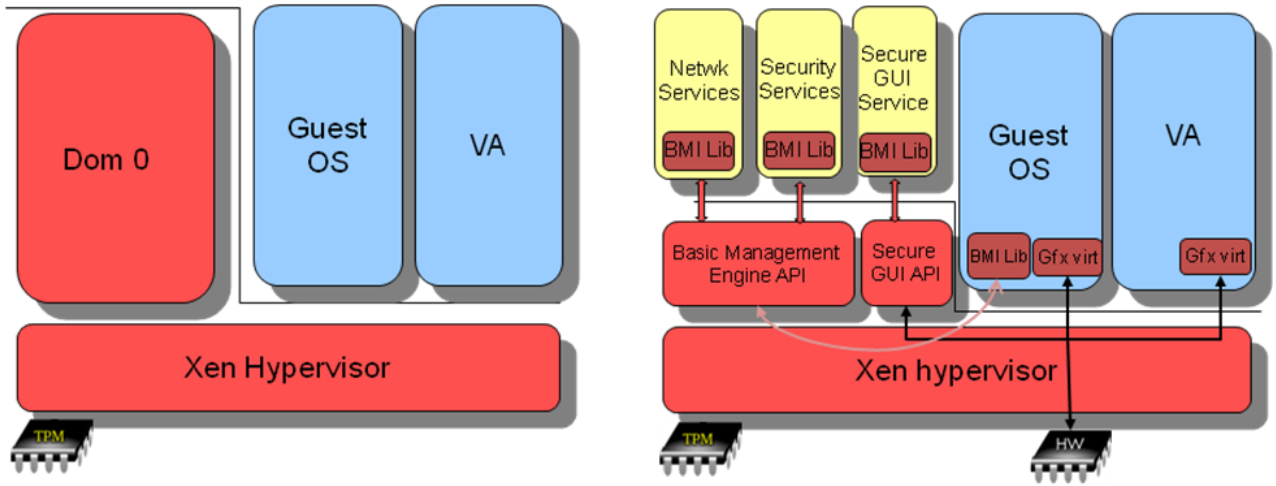
- Sichere, parallele Ausführung mehrerer OS und / oder Applikationen
- Reporting-Funktionen fuer virtualisierte Umgebungen, Attestation/Sealing
- OpenTC Vorstudie: „Corporate Computing at Home“
- Risikoreduktion durch Isolation und Disaggregation



hp invent

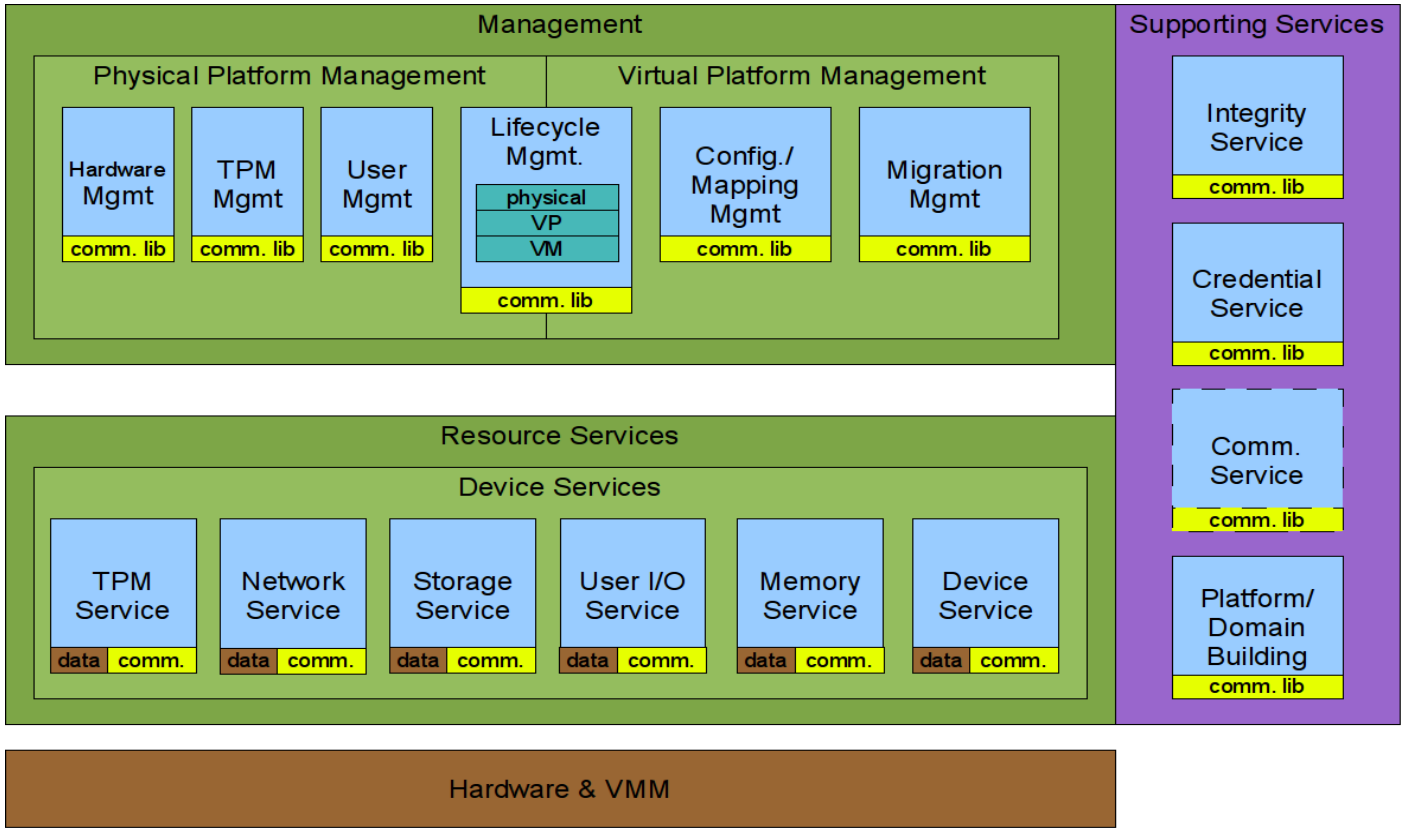
Disaggregation von Sicherheitsservices: Beispiele

- Dom Builder VM fuer Management des physikalischen Speichers
- Grafik-VM: Treiber ausserhalb Dom0, DirectX, PCI Pass-Through
- Basic Management for Security Interface (BMSI)
  - Lifecycle-Management fuer VMMs, Interface fuer HW TPM



hp invent

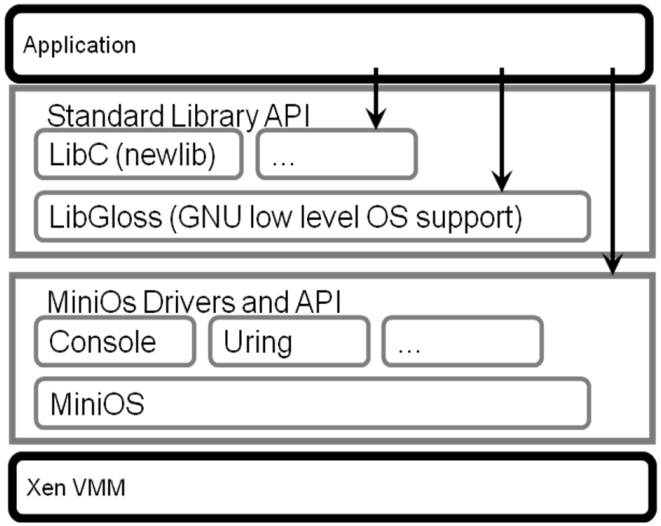
Services fuer vertrauenswürdige Virtualisierungs-Plattformen

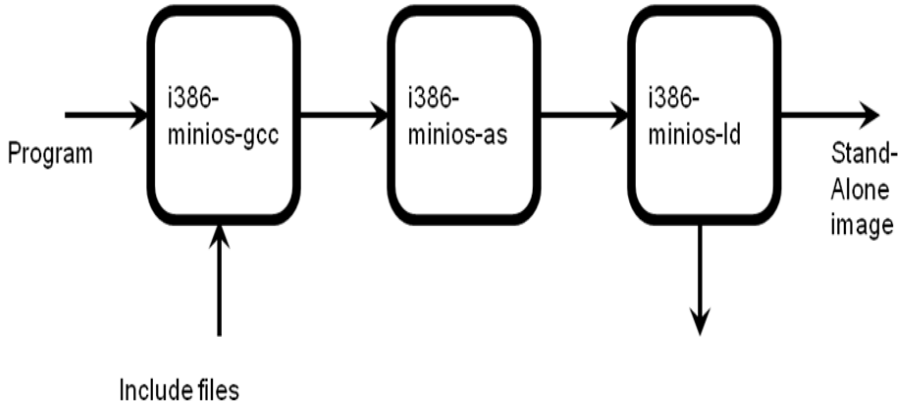


hp invent

Mini / Library OS

- Support fuer generische Services
  - Anlehnung an Mikro-Kernel Architekturen
  - Reduktion: ~100 kLOC fuer Service statt 1– 10 MLOC fuer OS
  - libc – Untermenge (*newlib),* Xen–spezifische Toolchain
  - Experimentell: Kapselung von Treibern (Ethernet)
  - Hauptaufgabe: inter-Domain Kommunikation

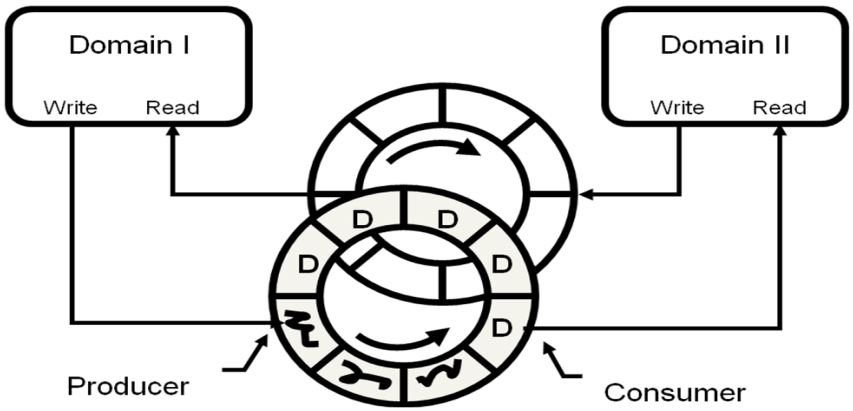




hp invent

Inter-Domain Kommunikation

- Alternative zu TCP/IP Inter-VMM Kommunikation unter Xen
  - Bibliothek, shared memory – Ringpuffer, File I/O API
- Paradigma: Xen Paravirtualisierungs-API
  - Keine Veränderung des Xen-VMMs erforderlich
  - Setup/ Synchronisation über XenStore
    - Adressierung per Domain-Identifikatoren, ähnlich sockets
    - Unterstuetzung fuer IPC / IDC Policies
  - Linux-Support: Kernel-Modul, erlaubt Prozesszugriff auf comm-API

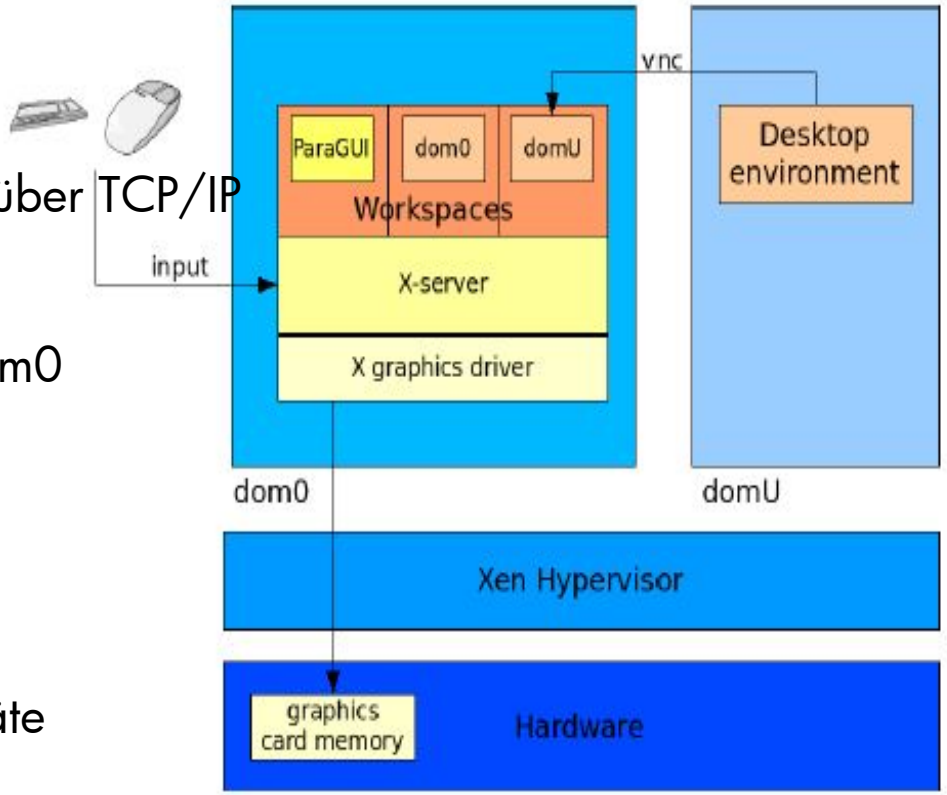


hp invent

Display – Virtualisierung (1)

Problemfeld: Trusted Path / Trusted I/O

- Prototyp 1: VNC -- basiert
  - (-) Transport der Grafikdaten über TCP/IP
  - (-) Abhängigkeit von X-Server
  - (-) Treiber und X-Server in Dom0
- Prototyp 2: sGUI – Domäne
  - (+) device – basiert
  - (+) Berücksichtigt Eingabegeräte

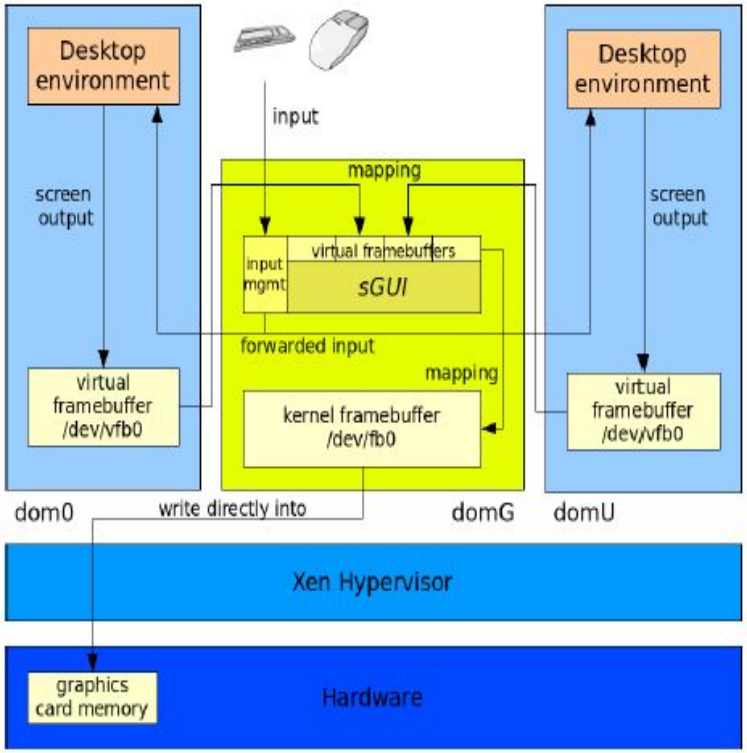


hp invent

Display – Virtualisierung (2)

Disaggregation der Graphik–Funktionen

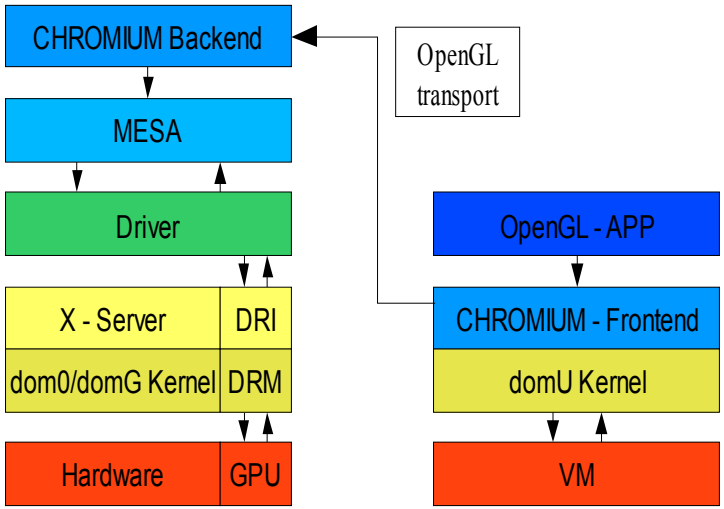
- Dedizierte Graphik – Domain
  - Kapselung Graphiktreibers
    - Virtualisierter Framebuffer
  - Kapselung sGUI-Komponenten
    - Tastatur / Maus
  - (+) device – basiert
  - (-) kein Zugriff auf Funktionen fuer Hardware – Beschleunigung
    - Essentiell fuer Windows Vista/ Aero (DirectX)
  - (-) Kapselung unzureichend (DMA – Zugriff der Graphik – Domäne)



hp invent

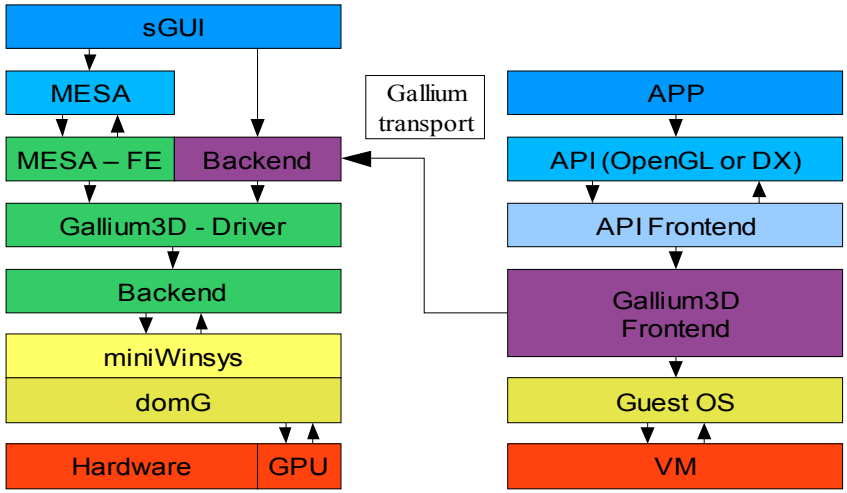
Display – Virtualisierung (3)

OpenGL



OpenGL Virtualisierung fuer Xen

OpenGL und DirectX

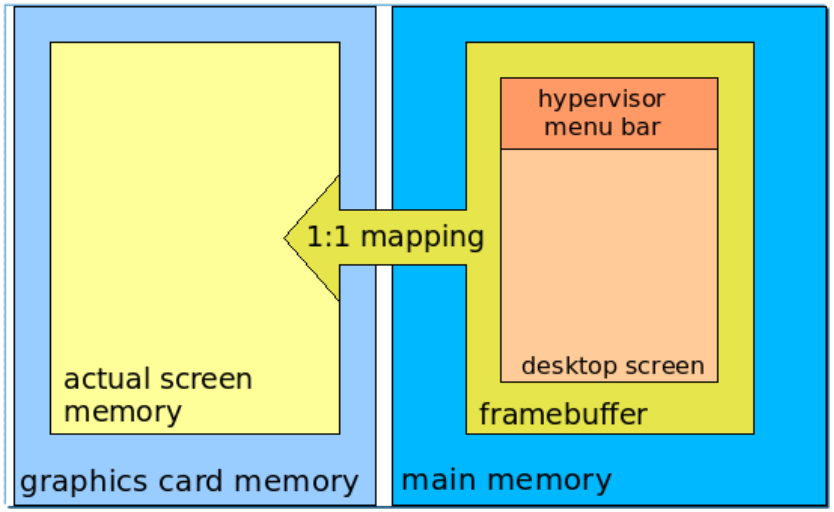


Gallium GPU Virtualisierung fuer Xen

- Gallium: Abstraktion von GPU-spezifischen Instruktionen
- Implementierbar fuer Xen und L4 Mikrokernel
- (Pass – trough Problem: Legacy Video BIOS Unterstützung)

hp invent

Display – Virtualisierung (4)

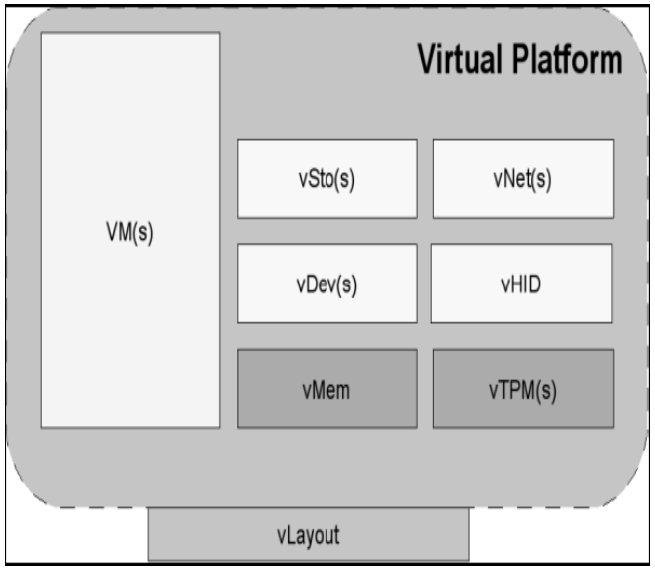


- Trennung der I/O – Bereiche durch IOMMU (Intel)
- Policy-kontrolliertes Overlaying, Alpha-Blending, Window-Labelling
- Sichere Trennung von Management- und User-Elementen

hp invent

Weitere Aktivitäten

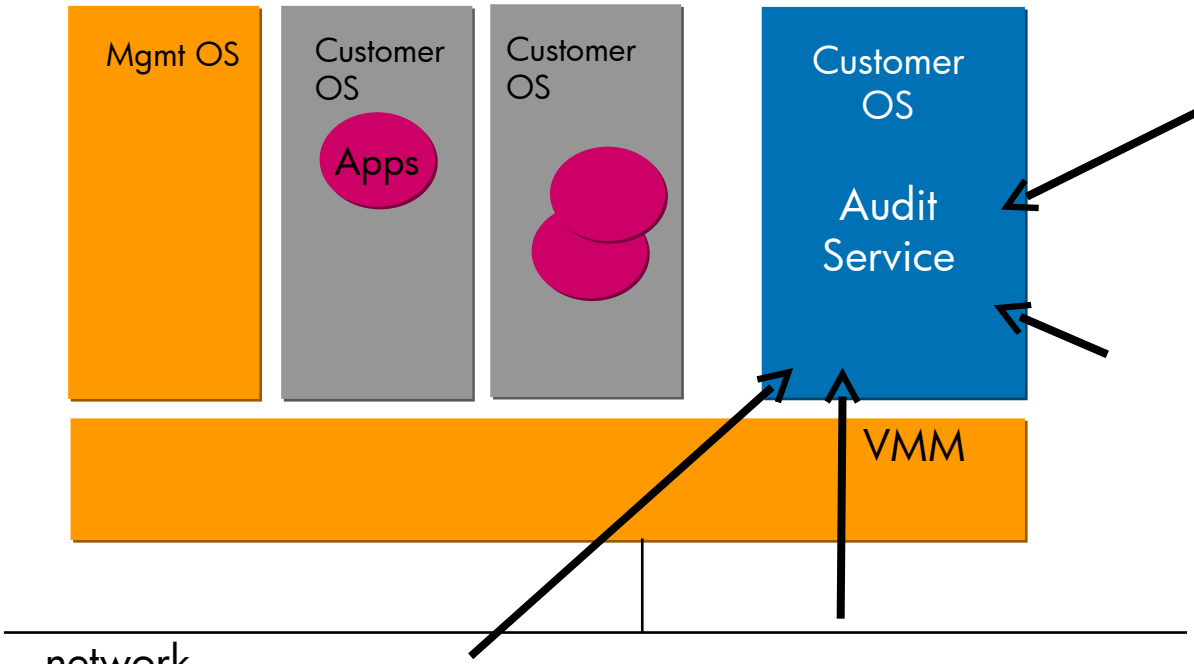
- Trusted Virtual Domains“
  - Cluster von vertrauenswürdigen virtuellen Plattformen
  - Netzwerkzugang abhängig von Softwarekonfiguration und Policies
  - Abbildung auf VLan-Tagging (lokal) und IPSec (Internet)
- Test und Validierung von Virtualisierungssoftware
  - Ex ante (Black Box / White Box Testing)
  - Fehlende (semi) formale Spezifikation
    - D.h., keine Verifikation im strengen Sinne
    - Jedoch: Verbesserung der Softwarequalität
- Management – Unterstützung
  - PKI, Metriken, Installation und Update
- Virtual Platform Enforcement Services
- Trusted Channels



hp invent

Cloud Data Centers
Audit /Assurance

Modellbasierte Auditing-Anforderungen



Sicherheits- (Audit-) Services getrennt von Management und User Space

Can collect and report metrics showing what OSs are running, how they booted etc…

hp invent

Mögliche Entwicklungen

- Hypervisor und Virtualisierungslayer als integraler Teil von Distributionen oder Hardware?
  - Basismechanismus fuer OS – Isolation
  - Generische Unterstützung fuer Trennung von Benutzerrollen
  - Herausforderung: Plattformzertifikate
- Platformcharakteristiken als Zugangskriterium fuer Services und Netze?
  - Remote Attestation fuer technische Eigenschaften und Policies
  - Lokale und verteilte “trust domains” mit gemeinsamen Regeln und Enforcement-Mechanismen
  - Haftbarkeitsverschiebung durch service-spezifische VMs
- Teilautomatisierte Unterstützung zum Nachweis von “due diligence” beim ICT management?
- Beschränkung von TC-Einsatz auf kooperative Szenarien?

hp invent

Vertrauen und Offenheit

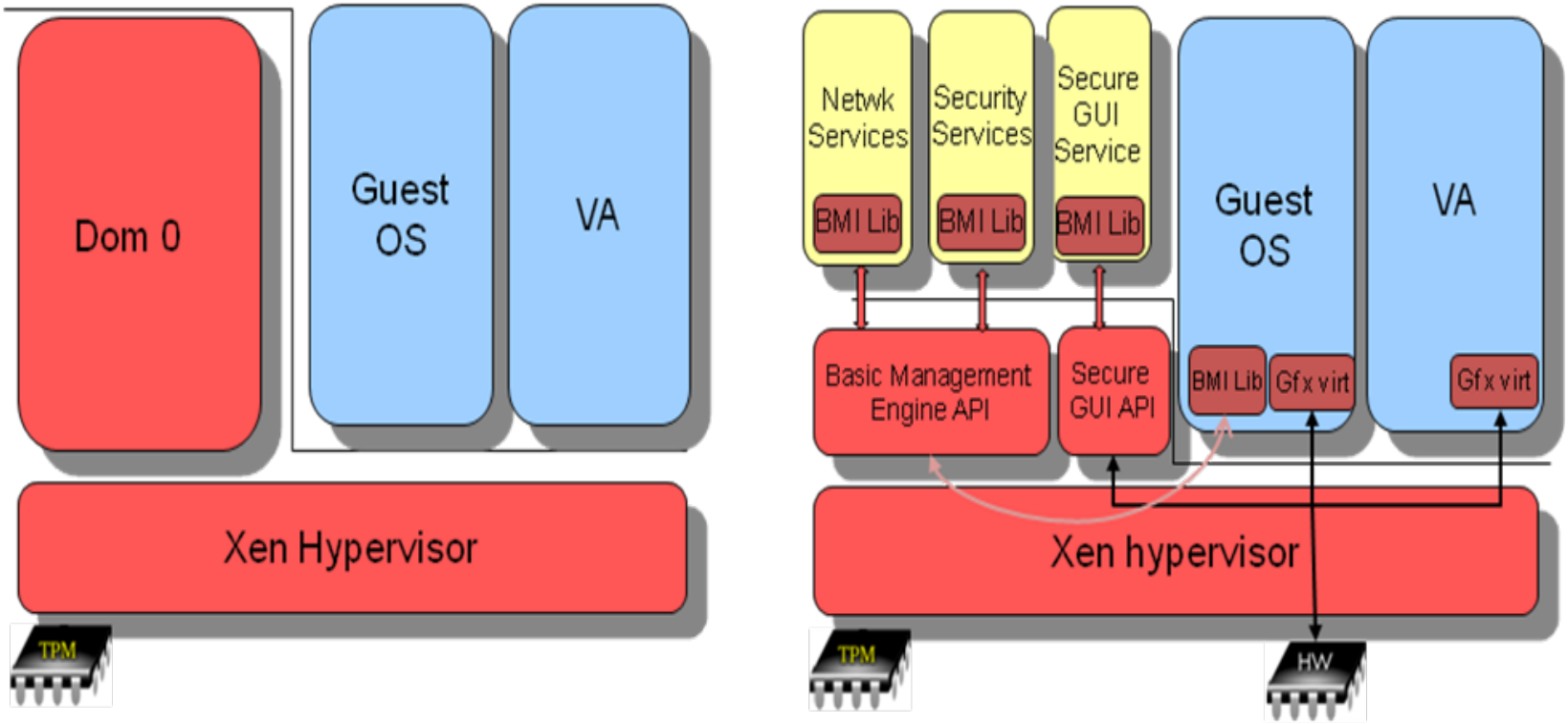
- Vertrauenswuerdigkeit von Software sollte überprüfbar sein
  - Publikation der Quellen notwendig, jedoch nicht hinreichend
    - Open Source Lizensierung nicht notwendig!
    - Dynamik von OSS stellt Problem fuer Zertifizierung dar
- Validierungs- und Testergebnisse sollten replizierbar sein
  - Offenlegung von Methodologie und Werkzeugen
- Alternative: Vertrauen durch Institutionalisierung und Branding
  - Expertenurteil oder automatische Beweise als vertrauensbildende Massnahmen?
  - Nagelprobe ist das praktische, beobachtbare Verhalten von ICT
  - Verstehbarkeit als Voraussetzung von Erwartung?

hp invent

Danke fuer Ihre Aufmerksamkeit!

Backup Slides

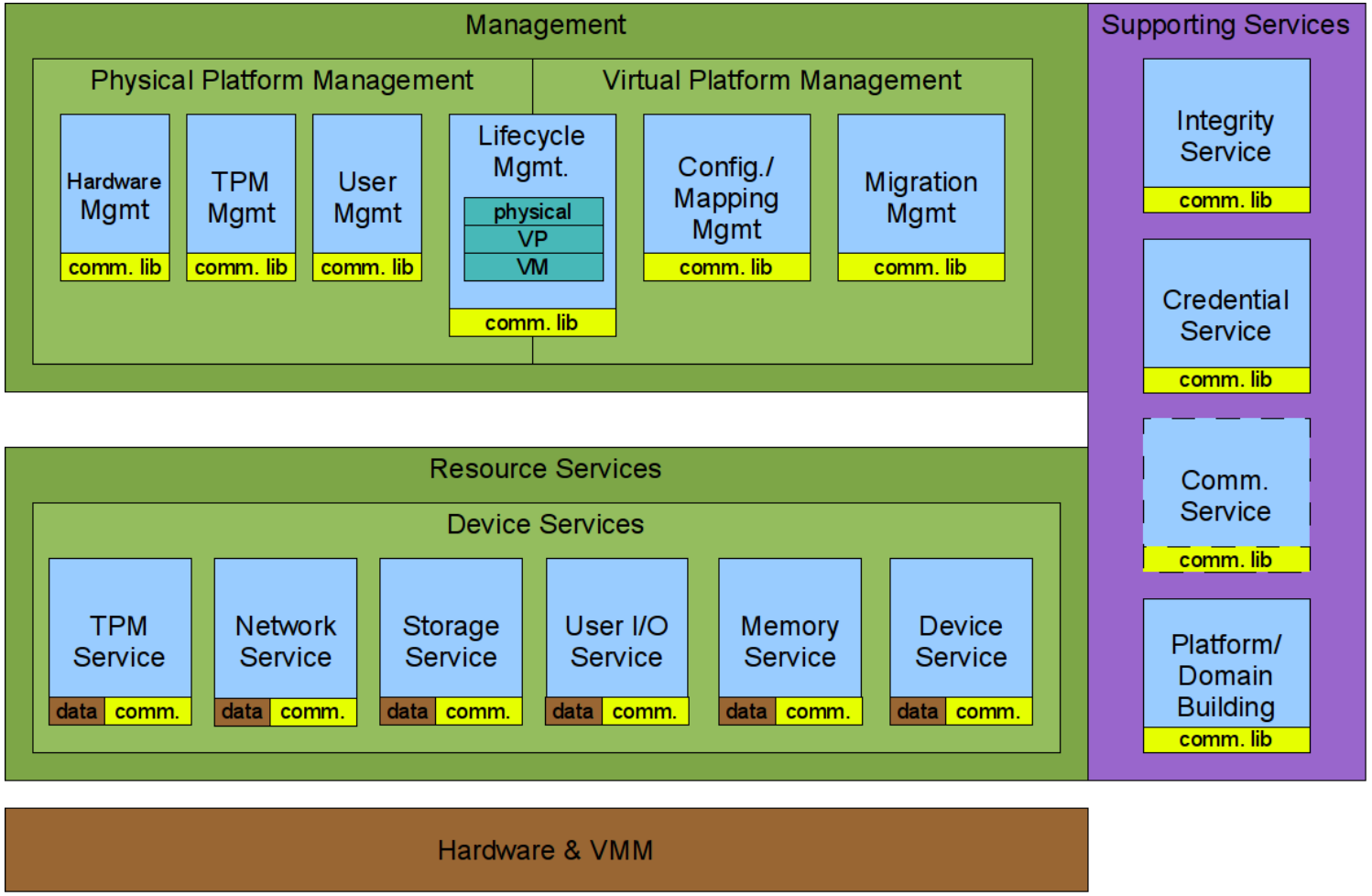
TV architecture



Trusted Computing Base for robustness and security guarantees

hp invent

Platform Core Services



hp invent