Verschlußsachen

amtlichen Stelle oder auf deren Veranlassung eingestuft.

(2) Eine Verschlußsache ist

1. STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,
2. GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,
3. VS-VERTRAULICH, wenn die Kenntnisnahme durch

§4 Abs. 2, Sicherheitsüberprüfungsgesetz (SÜG)

secunet Security Networks AG

Betriebssysteme für hohen Schutzbedarf: Anforderungen und Architekturkonzepte

München, 04. Dezember 2008

Alexander Senier

Motivation

- Kenntnisnahme hoch eingestufter Verschlußsachen (VS) durch Unbefugte stellt gravierendes Risiko dar
- Effiziente Verarbeitung durch moderne IT-Systeme jedoch unerlässlich
- Noch kritischer: gleichzeitige Verarbeitung unterschiedlich eingestufter Verschlußsachen
- Beispiele:
  - Bundeswehreinsatz im NATO-Kontext
  - Zugriff auf offene Informationen durch den Bundesnachrichtendienst
- **Zur sicheren, gleichzeitigen Verarbeitung von unterschiedlich eingestuften VS-Daten wird eine geeignete Betriebssystemplattform benötigt!**

Inhalt

- Sicherheitsanforderungen
- Architekturkonzepte
- Lösungsansätze

Inhalt dieses Vortrages sind nicht ...

- Klassische Multilevel-Security Systeme und Security Kernel
- Sicherheitsanforderungen innerhalb eines Geheimhaltungsgrades
- Aspekte zur Sicherheit niedrig eingestufter oder offener Informationen

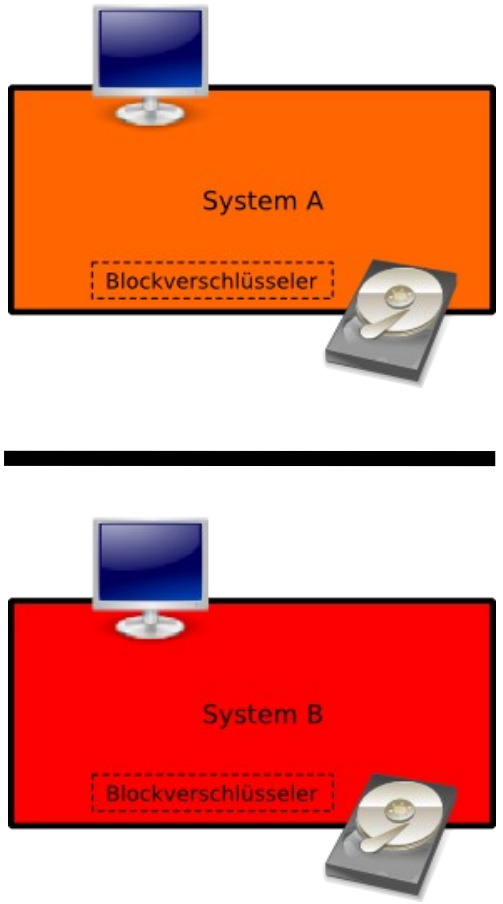
Sicherheitsanforderungen

- Gleichzeitige Verarbeitung unterschiedlich eingestufter Verschlußsachen stellt hohe Sicherheitsanforderungen:
  - **Vertraulichkeit**: Die Kenntnisnahme von Verschlußsachen durch Unbefugte ist ausgeschlossen.
  - **Integrität**: Es wird sichergestellt, dass Verschlußsachen unverändert und vollständig sind.
  - **Verfügbarkeit**: Der berechtigte Zugriff auf Verschlußsachen wird sichergestellt.
- **Herkömmlichen Betriebssystemen kann man nicht vertrauen, unterschiedlich eingestufte VS-Daten sicher zu verarbeiten!**

Architekturkonzepte

Mögliche Lösung: Hardwaretrennung

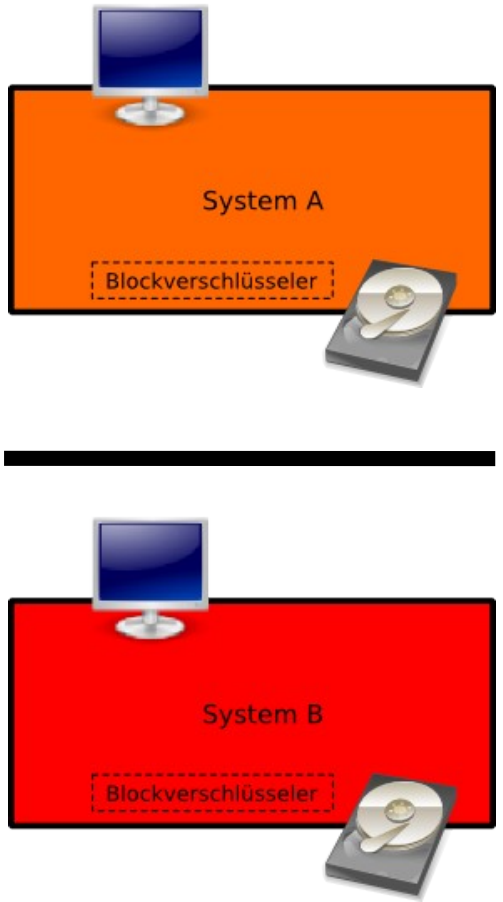
- Jede Einstufung wird auf einem vollständig getrennten System verarbeitet.
- Beispiel: Workstation mit Blockverschlüsselung



Architekturkonzepte

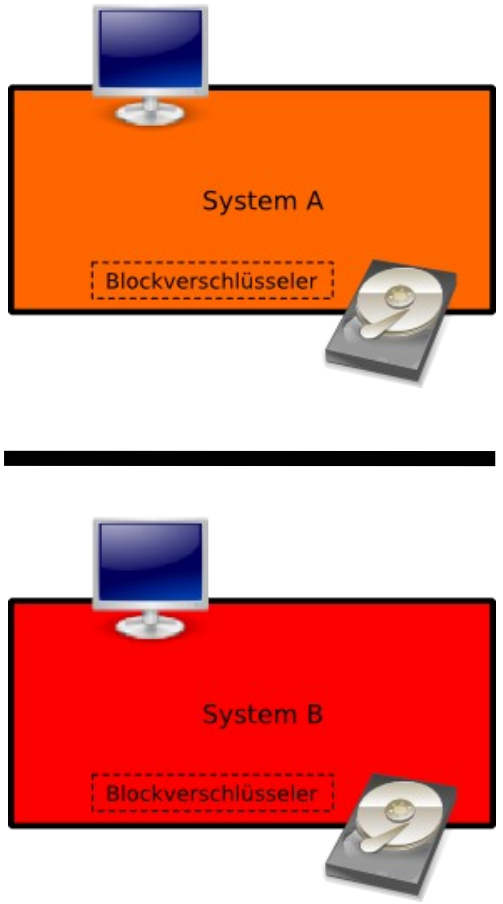
Nachteile der reinen Hardwaretrennung

- **Riskant:** Kopplung von Systemen
- **Teuer:** Hardware, Wartung, Transport, Energie, Platz
- **Ineffizient**: keine automatisierte Datenübergabe, mehrere Workstations
- **Beschränkt:** geringe Mobilität, hohe Rüstzeit
- **Hardwaretrennung ist nur eingeschränkt nutzbar – besser ist eine sichere, gleichzeitige Verarbeitung von VS-Daten auf *einem* System!**



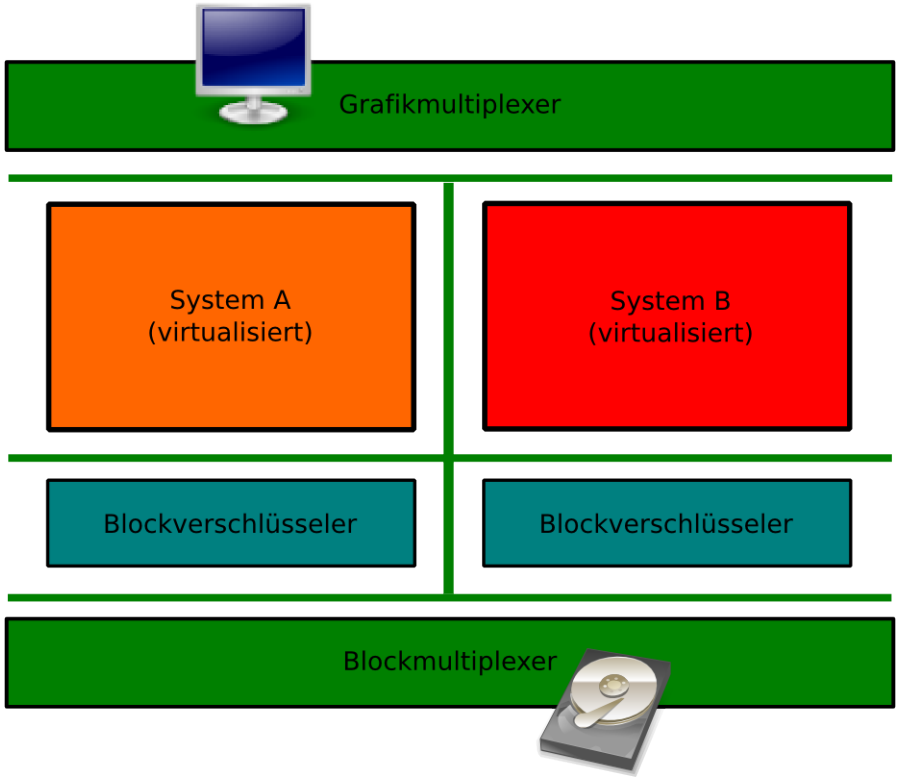
Architekturkonzepte
Sicheres Betriebssystem

- Ein sicheres Betriebssystem erzwingt die **Separierung** verschiedener **Komponenten** und die **sichere Ressourcenzuordnung** entsprechend einer Sicherheitspolitik.
- Dafür ist eine **sehr kleine Trusted Computing Base** (TCB) notwendig.



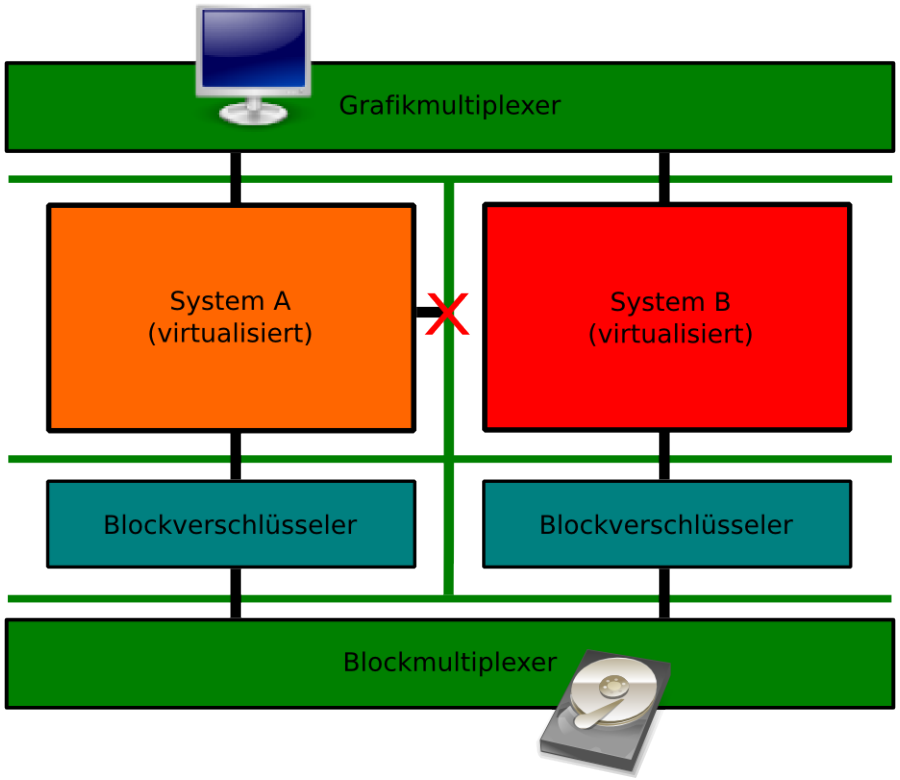
Architekturkonzepte
Komponenten

- Sehr kleine, vertrauenswürdige Anwendungen
  - Sichere Multiplexer
  - Trusted Wrappers
- Virtuelle Maschinen
  - Ausführung gängiger Betriebssysteme
  - Nutzung von Treibern



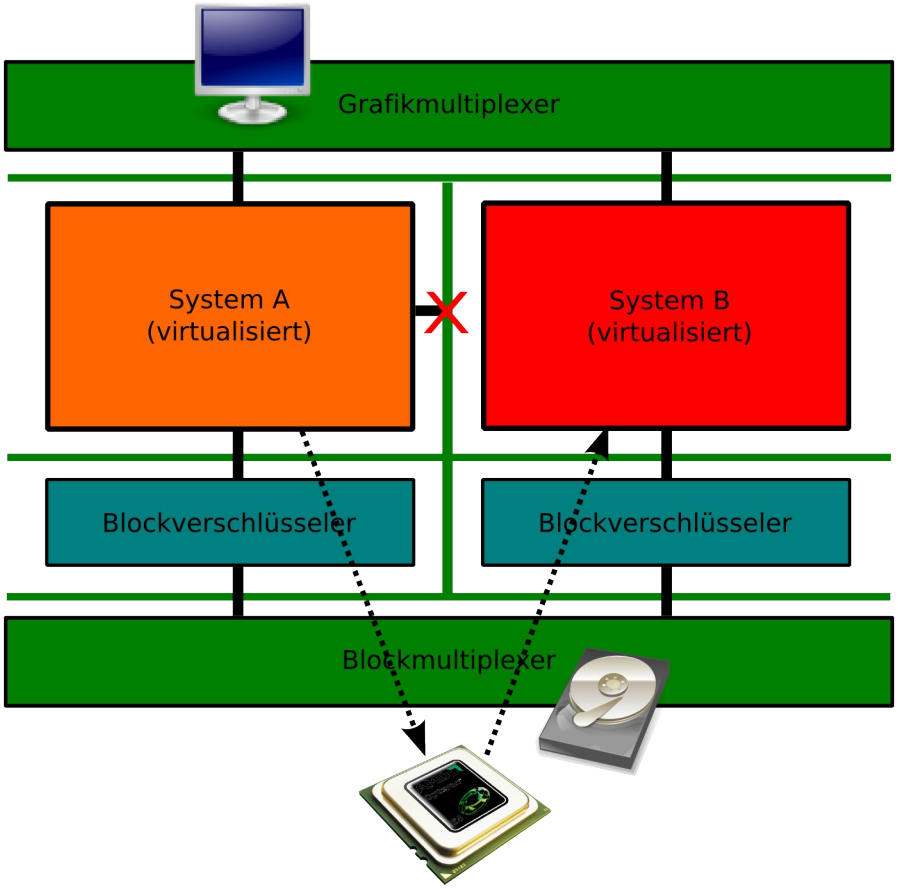
Architekturkonzepte
Separierung

- Kontrolle des Informationsflusses zwischen Komponenten eines Systems entsprechend einer Sicherheitspolitik
- Vollständige Unterbindung von verdeckten Datenkanälen (*covert storage channels*)
- Begrenzung von verdeckten Timingkanälen (*covert timing channels*) auf ein angemessenes Maß



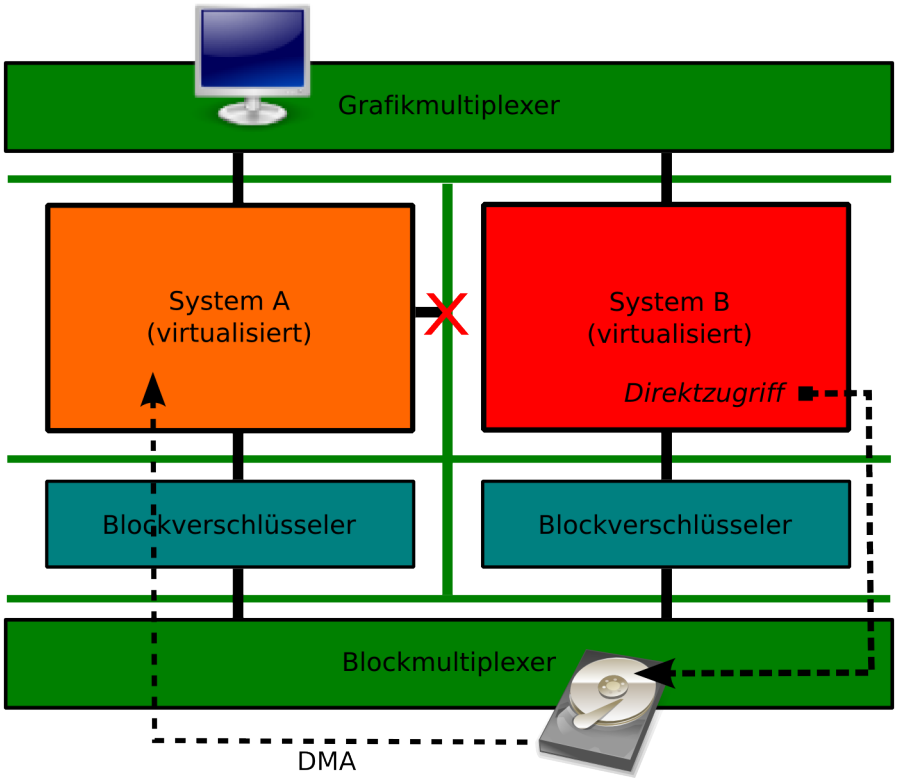
Architekturkonzepte
Verdeckte Kanäle

- **Verdeckter Kanal**: nichtautorisierter Kommunikationsweg in einem System, durch dessen Nutzung die Sicherheitspolitik verletzt wird
- Auch in der Praxis relevant:
  - Extraktion von Schlüsselmaterial, Demaskierung anonymisierter Verbindungen, Übertragung von Informationen, ...
- Prinzipiell auch Virtuelle Maschinen, Sandboxen, etc. angreifbar



Architekturkonzepte
Sichere Ressourcenzuordnung

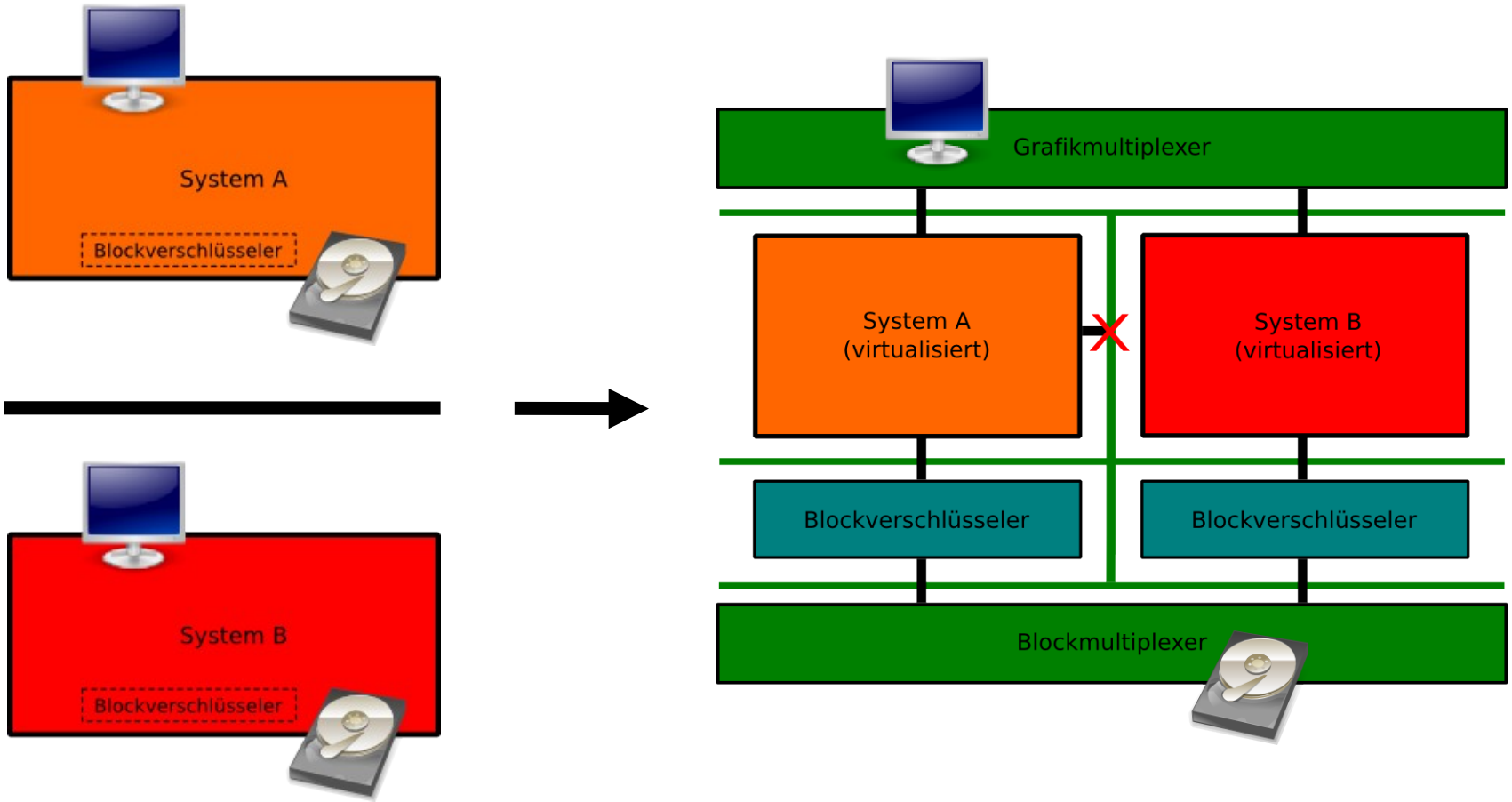
- Eindeutige und nicht-umgehbare Zuordnung von Ressourcen zu Komponenten
- Ressourcen: Menge aller Hardware, Firmware, Software und Daten, die durch ein System ausgeführt, benutzt, erzeugt, geschützt oder exportiert werden
- Aufrechterhaltung des sicheren Systemzustandes, Durchsetzung der Sicherheitspolitik, Separierung



Architekturkonzepte
Sehr kleine Trusted Computing Base (TCB)

- Sehr klein
  - Sichere Multiplexer und Trusted Wrapper sind die kritischsten Elemente der TCB
  - Minimalisierung von Architektur, Design und Funktionalität ist unerlässlich
- Trusted
  - Trusted = Trustworthy?
  - Entwicklungsprozess muss Vertrauenswürdigkeit der Software sicherstellen
  - Einsatz sicherer Programmiersprachen wie Ada
  - Correctness-by-Construction und formale Verifikation kritischer Elemente
  - Sehr strenge Qualitätssicherung und hohe Qualität der **gesamten TCB**

Architekturkonzepte
Zusammenfassung



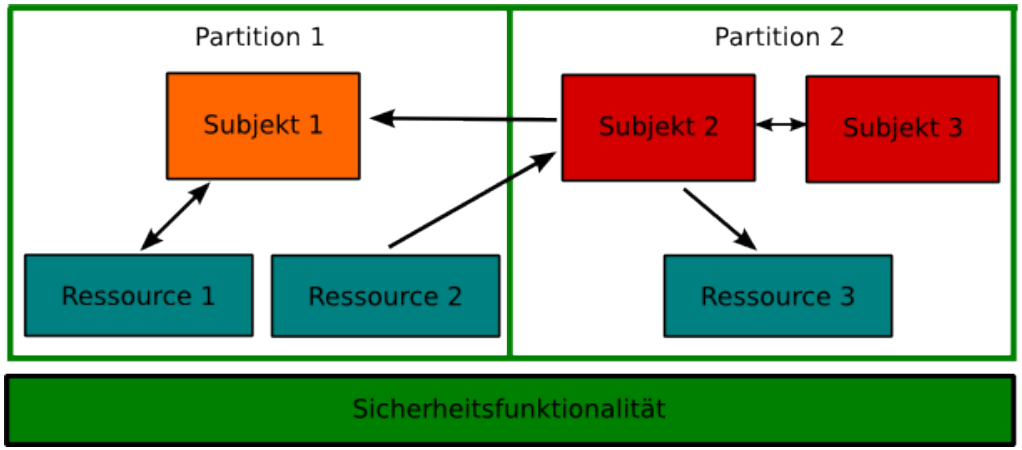
Lösungsansätze

Separation Kernel Protection Profile (SKPP)

- Durch die NSA erstelltes Protection Profile
- Sicherheitsanforderungen, funktionale Anforderungen und Assurance Anforderungen für die Klasse der Separation Kernel
- Robuste Grundlage für Dienste und Anwendungen in kritischen Systemen
- Innerhalb geeigneter Sicherheitsarchitektur gedacht für:
  - Verteidigung
  - Luftfahrt
  - Finanzwesen
  - andere sensible Bereiche

Lösungsansätze
Separation Kernel

- Aufgabe von Separation Kerneln:
  - Partitionierung von Subjekten und Ressourcen in Äquivalenzklassen bezüglich einer Sicherheitspolitik
  - Kontrolle des Informationsflusses innerhalb und zwischen Partitionen



Lösungsansätze
Anforderungen aus dem SKPP

- Betrachtung von Separation Kernel **und** Hardwareplattform
- Informationsflusskontrolle, Isolation von Ressourcen, vertrauenswürdige Initialisierung, vertrauenswürdige Auslieferung, vertrauenswürdige Wiederherstellung, Auditfunktionalität
- Design, Architektur und Funktionalität bezüglich Größe und Komplexität minimal
- Betrachtung der verwendeten Prozesse und Werkzeuge
- Analysen durch die NSA (verdeckte Kanäle, Kyptoalgorithmen, Schwachstellen- und Penetrationsanalyse)

Lösungsansätze
Verfügbare Separation Kernel

- Bewertung von Separation Kerneln für eine Multilevel-Workstation auf PC
- Bisherige Beobachtungen:
  - Keine frei verfügbaren Systeme bekannt
  - Plattformen kommen meist aus der Avionik und sind auf Safety ausgerichtet
  - Folge: Kerneltreiber, unkontrollierte Reservierung von Interrupts, kein Schutz vor unautorisierten DMA-Zugriffen
  - PC (x86/amd64) ist selten die Primärplattform (eher PowerPC und ARM)
  - Ein System gegen SKPP evaluiert (allerdings auf PowerPC, ohne Gerätetreiber und ohne Virtualisierung)
- Untersuchung dauert noch an ...

Zusammenfassung

- Die gleichzeitige Verarbeitung hoch eingestufter VS-Daten stellt sehr hohe Anforderungen an die Sicherheit.
- Absicherung durch Hardwaretrennung ist möglich, aber nicht immer praktikabel.
- Besser: Betriebssystem mit sehr kleiner Trusted Computing Base, das starke Separierung und sichere Ressourcenzuordnung auf **einer** Hardware erzwingt.
- Auf einem Separation Kernel schaffen Sichere Multiplexer, Trusted Wrapper und Virtuelle Maschinen eine sehr starke Isolation unterschiedlicher Einstufungen.
- Der Entwurfs- und Entwicklungsprozess muss die Vertrauenswürdigkeit und sehr hohe Qualität der **gesamten** Trusted Computing Base sicherstellen.
- Einsetzbarkeit für Multilevel-Workstation auf PC wird zur Zeit untersucht ...

Literatur

- Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (Sicherheitsüberprüfungsgesetz – SÜG) vom 20. April 1994, zuletzt geändert durch Artikel 6 des Gesetzes vom 26. Februar 2008.
- Michael Hohmuth, Michael Peter, Hermann Härtig und Jonathan S. Shapiro. Reducing TCB size by using untrusted components — small kernels versus virtual-machine monitors (2004).
- U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP), Version 1.03, Information Assurance Dictorate (2007).
- John Rushby. Design and Verification of Secure Systems (1981).
- Onur Acıiçmez. Yet Another MicroArchitectural Attack: Exploiting I-cache (2007).