Noninterference in the Take-Grant Model for the seL4 Microkernel

Andrea Kuchar

INSTITUT FÜR INFORMATIK
DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
Lehr- und Forschungseinheit für theoretische Informatik

September 11, 2018

Überblick

Zusammenfassung

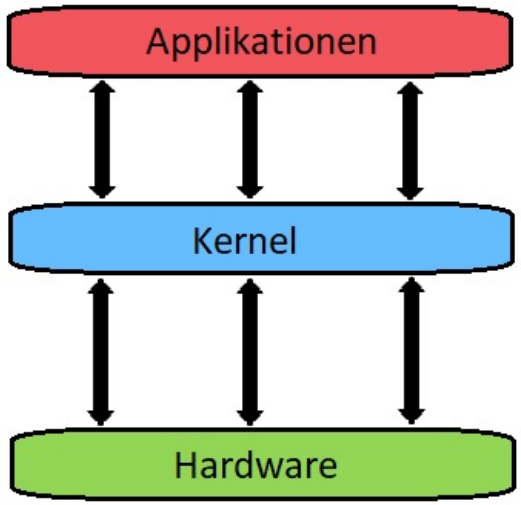
Ist die Spezifikation der seL4 Zugriffskontrolle stark genug ist, um die Noninterference-Eigentschaften an ihr zu zeigen?

Vorgehen:

- Analyse des Take-Grant-Protection Modells
- Erweiterung des Modells
- Zeigen der Noninterference-Eigenschaften an jeder der Systemoperationen

Motivation

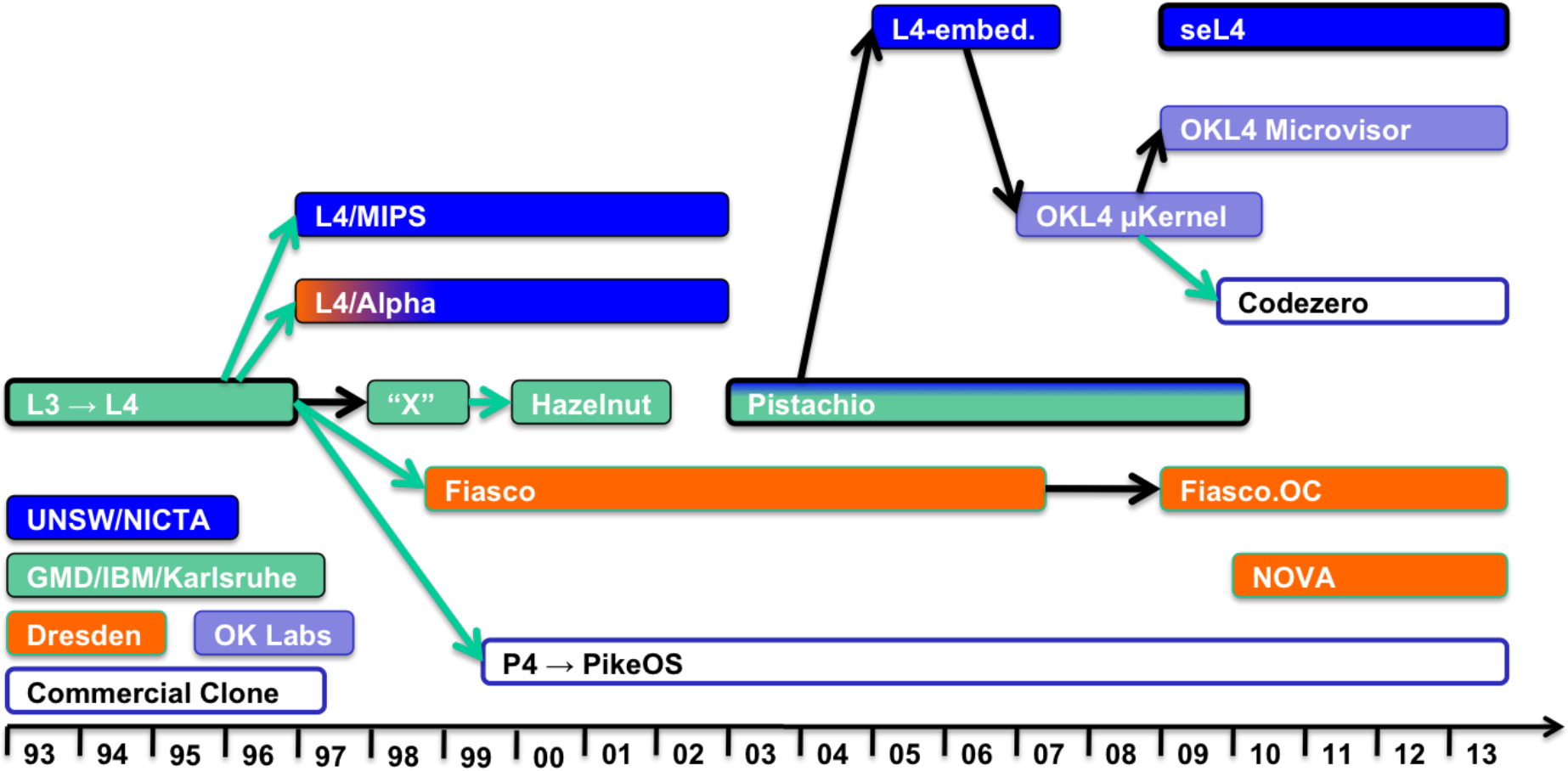
- Kernel = Schlüsselkomponente für sichere Systeme
- Zugriffsteuerung auf Hardwarekomponenten
- Fehler im Kernel kann die Sicherheit und Verlässlichkeit des kompletten Systems zum erliegen bringen.
- Monolithische Designs:
  - Große Menge Code
  - Integration weiterer Funktionen.
  - Folge: Grundlegend schwach durch größere Anfällgkeit für Bugs.



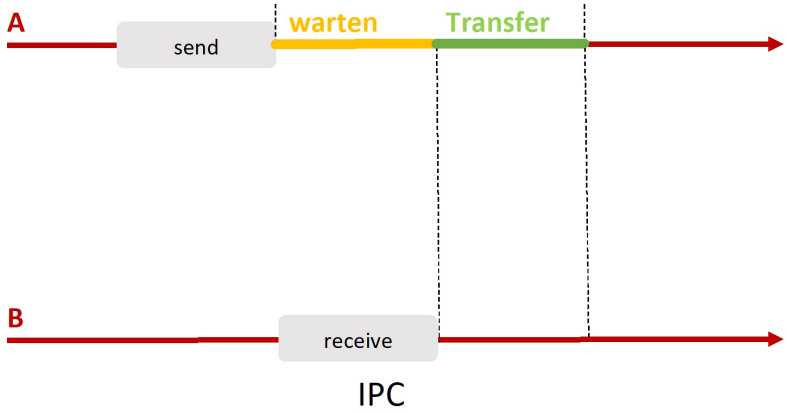
- Microkernel:
  Konzentration auf die fundamentalen Funktionen eines Kernels:
  z.B. Interprozesskommunikation, Scheduling, Speicherverwaltung
- Durch Microkernels: Fehleranfälligkeit verringern (weniger Code $\Rightarrow$ Fehlerfreiheit formell verifizierbar)

seL4

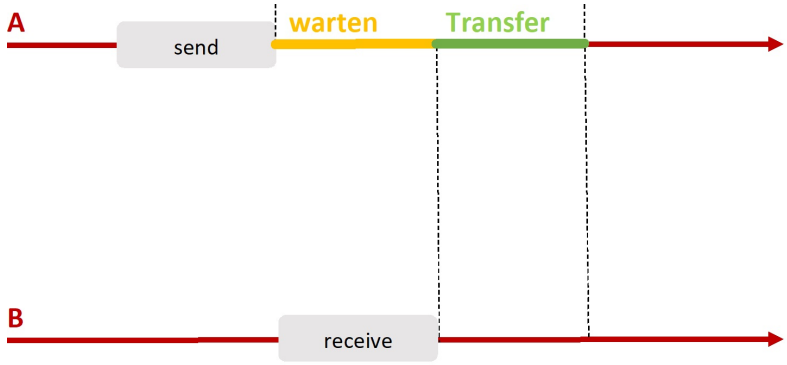
- In den 1990er Jahren entwickelt.
- Basiert auf dem L4 Microkernel.


L4-embed.
seL4
OKL4 Microvisor
OKL4 µKernel
L4/MIPS
L4/Alpha
Codezero
L3 → L4
"X"
Hazelnut
Pistachio
Fiasco
Fiasco.OC
UNSW/NICTA
GMD/IBM/Karlsruhe
NOVA
Dresden
OK Labs
P4 → PikeOS
Commercial Clone
93
94
95
96
97
98
99
00
01
02
03
04
05
06
07
08
09
10
11
12
13

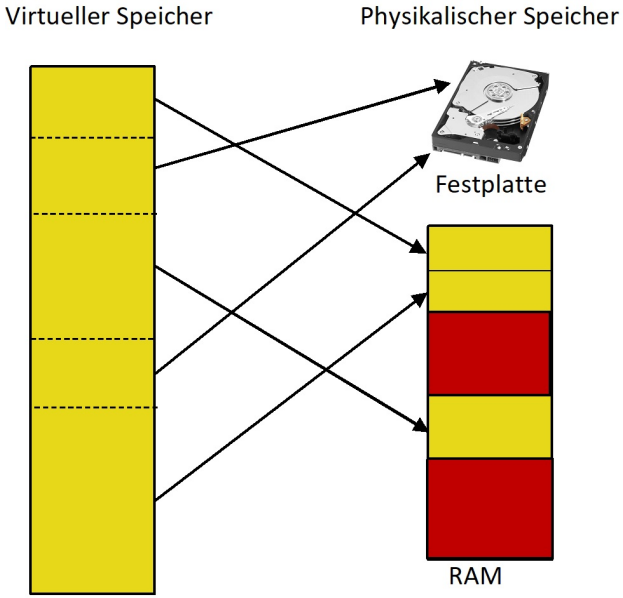
- In den 1990er Jahren entwickelt.
- Basiert auf dem L4 Microkernel.
- Stellt minimale Anzahl an services für Applikationen bereit.



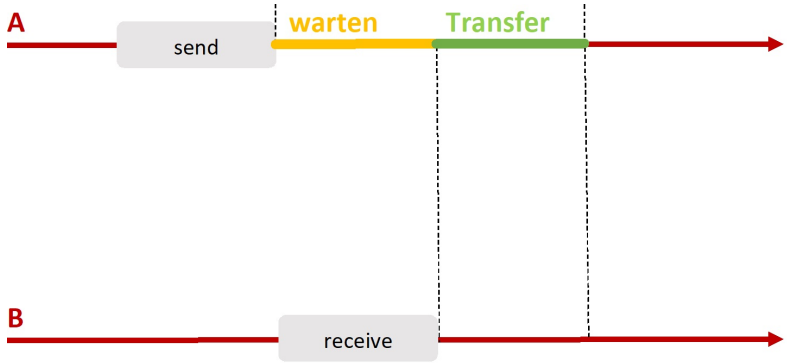
IPC



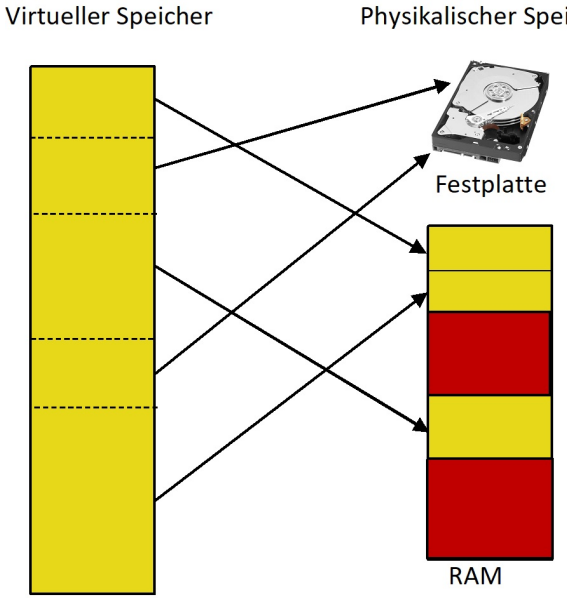
IPC



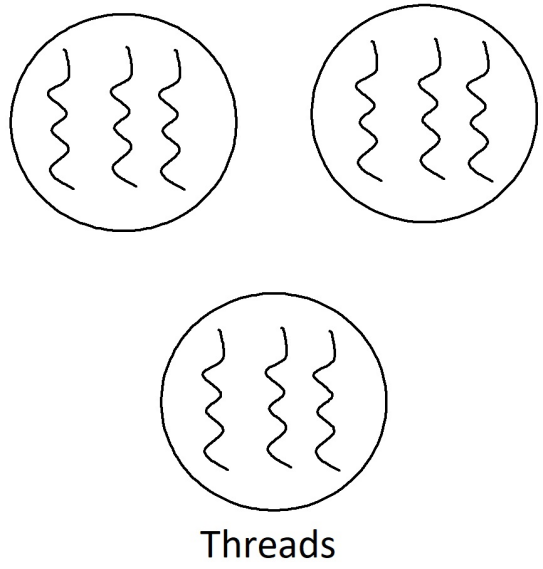
Speicherverwaltung



IPC



Speicherverwaltung

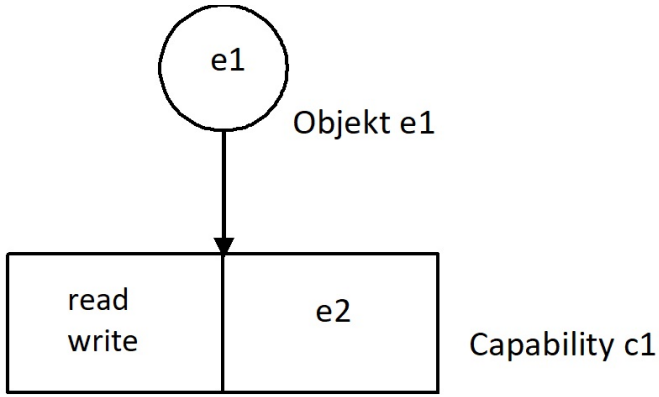


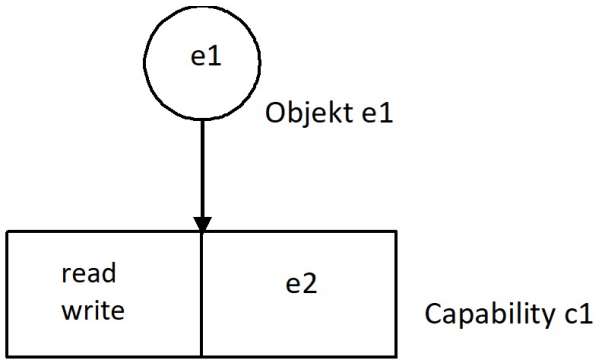
Threads

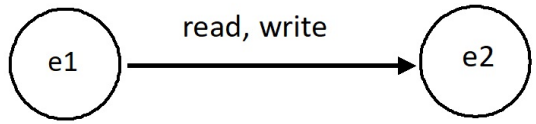
- In den 1990er Jahren entwickelt.
- Basiert auf dem L4 Microkernel.
- Stellt minimale Anzahl an services für Applikationen bereit.
- **Objekte:** implementieren jeweils die Abstraktion eines Services.

- In den 1990er Jahren entwickelt.
- Basiert auf dem L4 Microkernel.
- Stellt minimale Anzahl an services für Applikationen bereit.
- **Objekte:** implementieren jeweils die Abstraktion eines Services.
- **Capabilities:** von Applikationen benötigt, um einen Service zu nutzen.

- In den 1990er Jahren entwickelt.
- Basiert auf dem L4 Microkernel.
- Stellt minimale Anzahl an services für Applikationen bereit.
- **Objekte:** implementieren jeweils die Abstraktion eines Services.
- **Capabilities:** von Applikationen benötigt, um einen Service zu nutzen.
- Die Rechte `Read`, `Write`, `Grant` und `Create` können in den Capabilities enthalten sein.


e1
Objekt e1
read
write
e2
Capability c1


e1
Objekt e1
read
write
e2
Capability c1

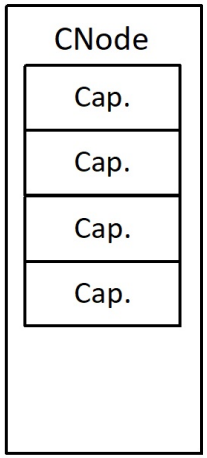

e1
read, write
e2

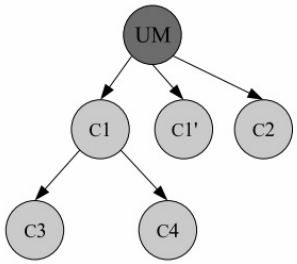
Kernel Objekte

- CNodes
- IPC Endpoints
- TCP
- Virtual Memory
- Interrupt Objects
- Untyped Memory

CNodes

- Lagern die Capabilities
- Erhalten feste Zahl an Slots
- Kernel konstruiert einen CDT (Capability Derivation Tree) zur Dokumentation der erstellten Capabilities und ihrer Verbindungen.





Blocks of Highlighted Text

Block 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Block 2

Pellentesque sed tellus purus. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum quis magna at risus dictum tempor eu vitae velit.

Block 3

Suspendisse tincidunt sagittis gravida. Curabitur condimentum, enim sed venenatis rutrum, ipsum neque consectetur orci, sed blandit justo nisi ac lacus.

Multiple Columns

Heading

1. Statement
2. Explanation
3. Example

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer lectus nisl, ultricies in feugiat rutrum, porttitor sit amet augue. Aliquam ut tortor mauris. Sed volutpat ante purus, quis accumsan dolor.

Table

Treatments	Response 1	Response 2
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Theorem

Theorem (Mass–energy equivalence)

$E = mc^2$

Verbatim

Example (Theorem Slide Code)

```
\begin{frame}
\frametitle{Theorem}
\begin{theorem}[Mass--energy equivalence]
$E = mc^2$
\end{theorem}
\end{frame}
```

Figure

Uncomment the code on this slide to include your own image from the same directory as the template .TeX file.

Citation

An example of the `\cite` command to cite within the presentation:

This statement requires citation [Smith, 2012].

References

John Smith (2012)

Title of the publication

Journal Name 12(3), 45 – 678.

The End