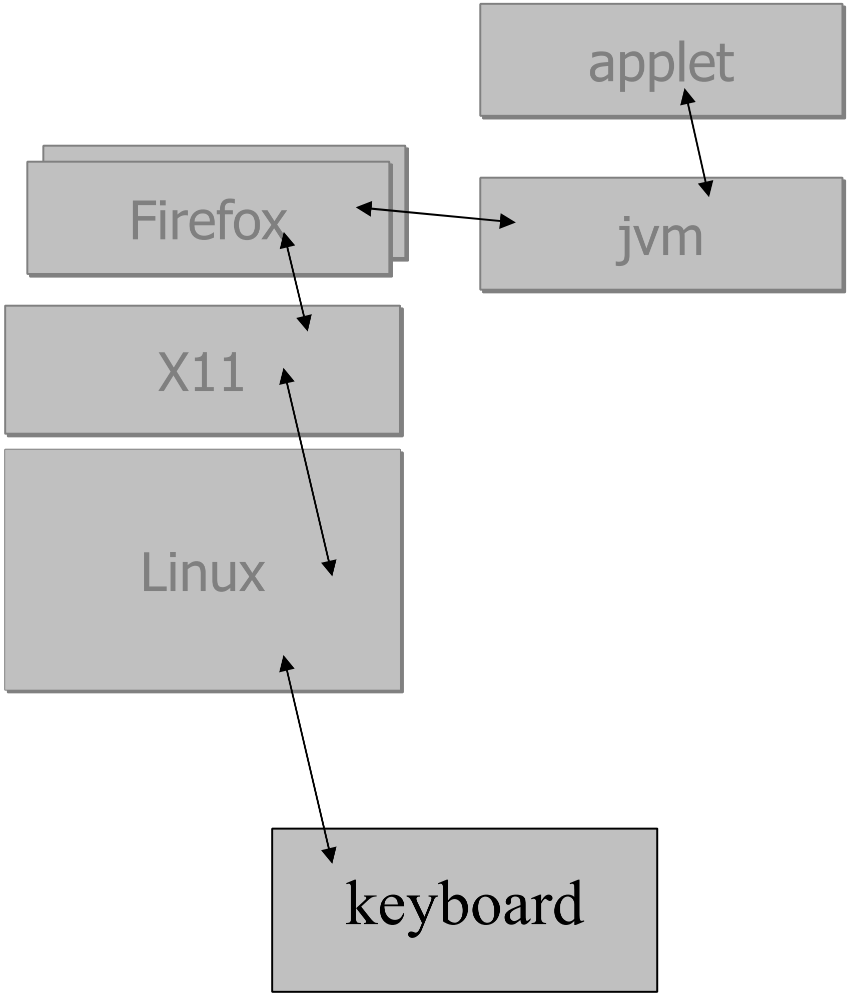
Mikrokerne und Virtualisierung als Basis sicherer Systeme

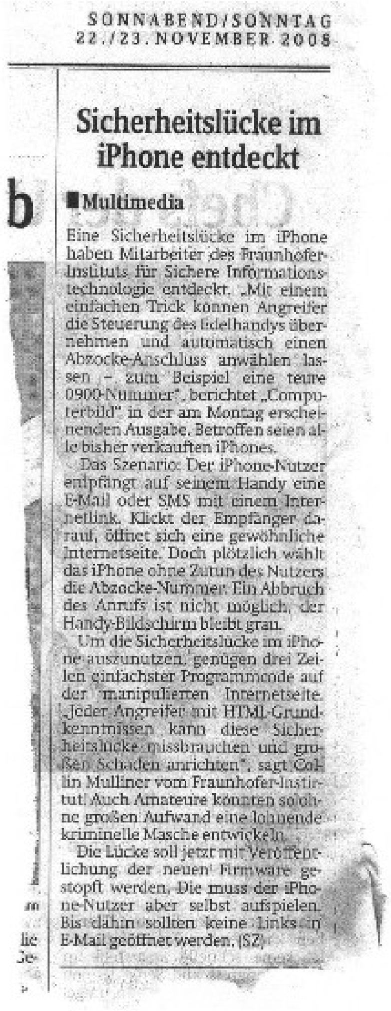
Hermann Härtig
Based on Work (and Slides) by Members of
TU Dresden : Operating Systems Group (TUD:OS)

Dezember 2008, UniBW&BSI, München

Motivation



Sächsische Zeitung, Nov 2008



SONNABEND/SONNTAG
22./23. NOVEMBER 2008

Sicherheitslücke im iPhone entdeckt

■Multimedia

Eine Sicherheitslücke im iPhone haben Mitarbeiter des Fraunhofer-Instituts für Sichere Informationstechnologie entdeckt. „Mit einem einfachen Trick können Angreifer die Steuerung des Edelhandys übernehmen und automatisch einen Abzocke-Anschluss anwählen lassen – zum Beispiel eine teure 0900-Nummer", berichtet „Computerbild" in der am Montag erscheinenden Ausgabe. Betroffen seien alle bisher verkauften iPhones.

Das Szenario: Der iPhone-Nutzer empfängt auf seinem Handy eine E-Mail oder SMS mit einem Internetlink. Klickt der Empfänger darauf, öffnet sich eine gewöhnliche Internetseite. Doch plötzlich wählt das iPhone ohne Zutun des Nutzers die Abzocke-Nummer. Ein Abbruch des Anrufs ist nicht möglich, der Handy-Bildschirm bleibt grau.

Um die Sicherheitslücke im iPhone auszunutzen, genügen drei Zeilen einfachster Programmcode auf der manipulierten Internetseite. „Jeder Angreifer mit HTML-Grundkenntnissen kann diese Sicherheitslücke missbrauchen und großen Schaden anrichten", sagt Collin Mulliner vom Fraunhofer-Institut. Auch Amateure könnten so ohne großen Aufwand eine lohnende kriminelle Masche entwickeln.

Die Lücke soll jetzt mit Veröffentlichung der neuen Firmware gestopft werden. Die muss der iPhone-Nutzer aber selbst aufspielen. Bis dahin sollten keine Links in E-Mail geöffnet werden. (SZ)

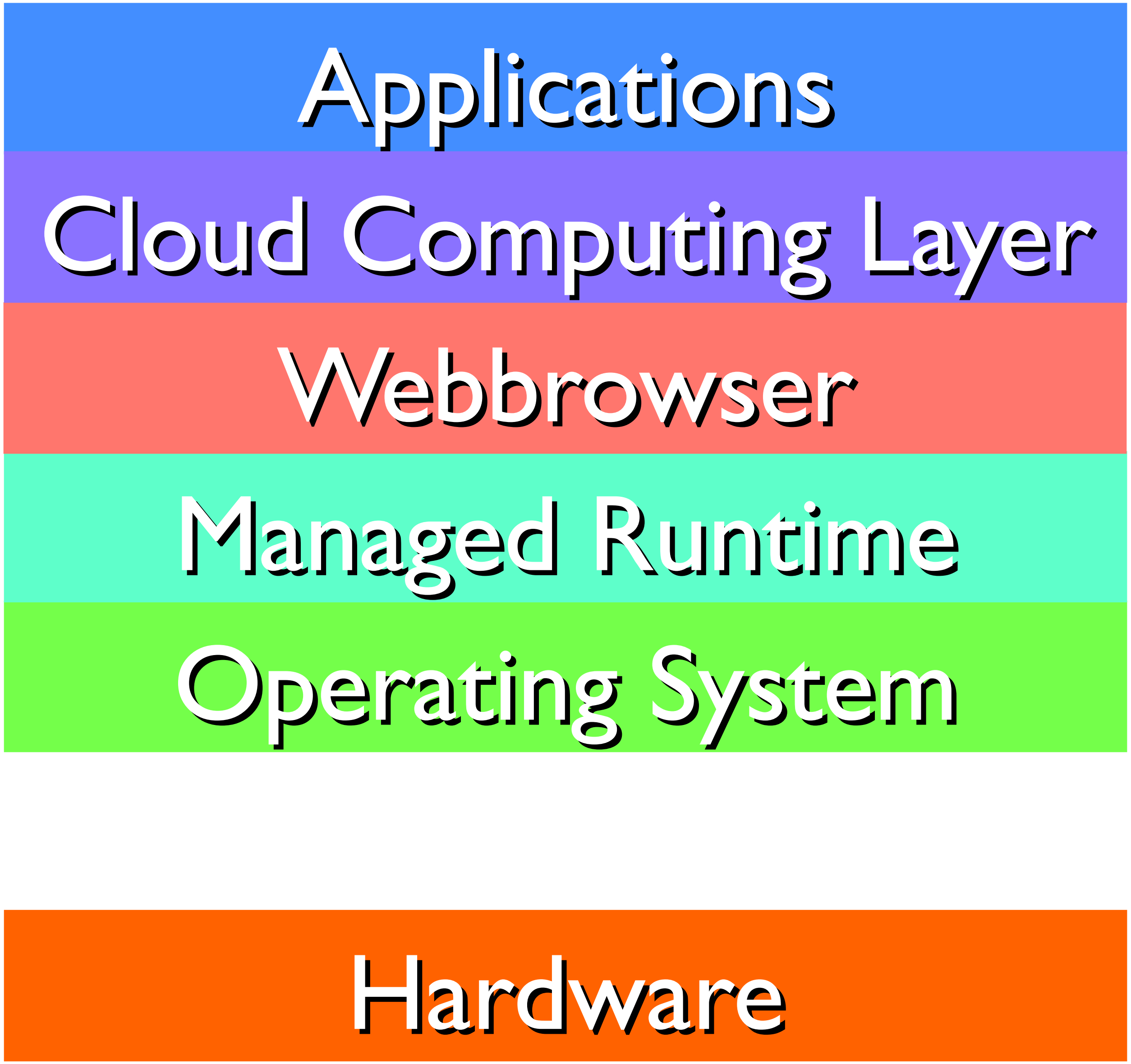
Simulated Situation:

- Cell Phone Platform
- Linux and Dialler
- Fully Compromised Linux
- Attempt to Dial 0900 xxx
- Dialler reliably shows number before dialing

Outline

- Virtual Machines and Micro-Kernels: Orthogonal and Complementary Technologies
- TUD:OS Propaganda
- Application Areas
- Where we Stand, What we Need

Getting … where ?



Applications

Cloud Computing Layer

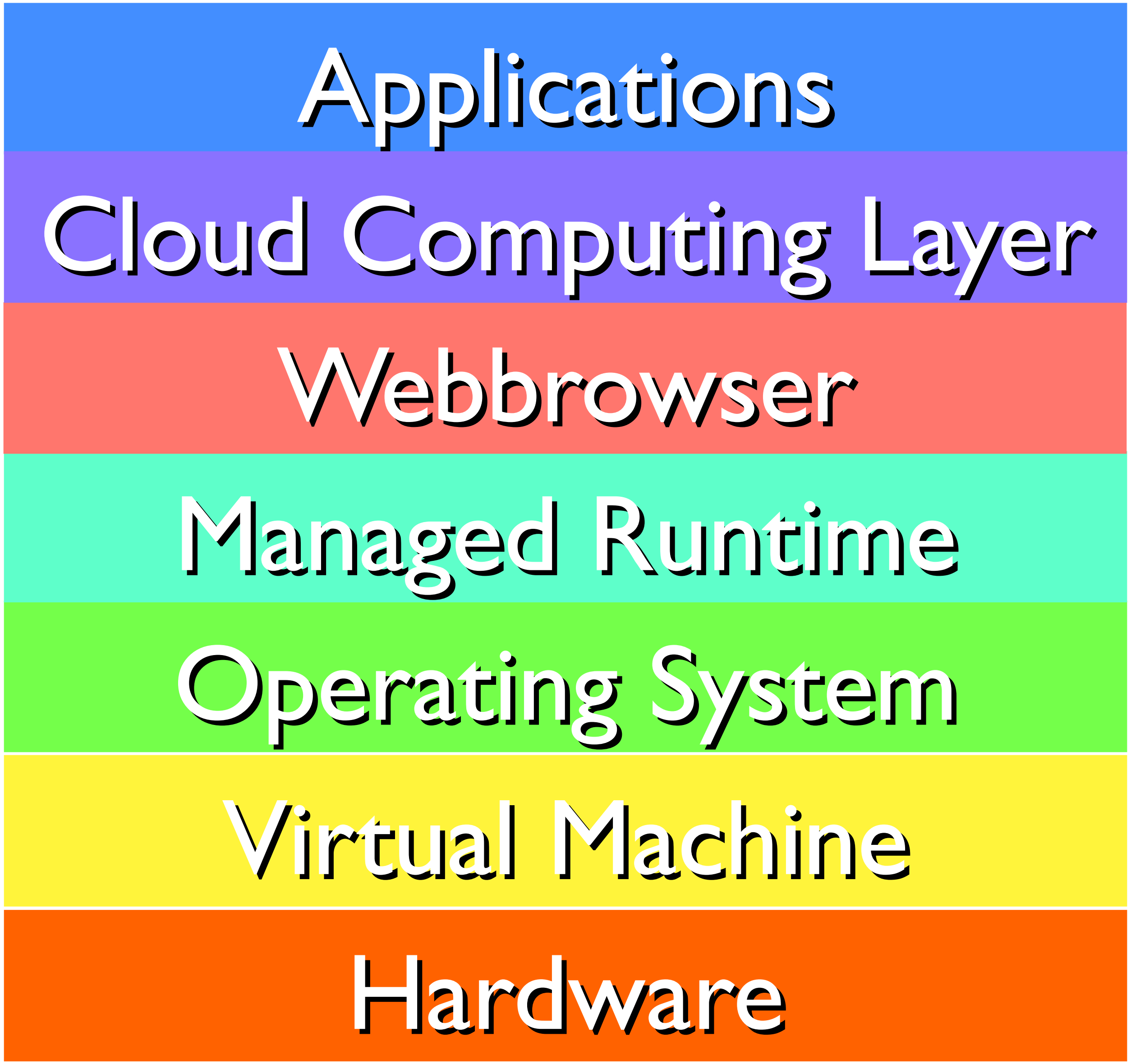
Webbrowser

Managed Runtime

Operating System

Hardware

Any Better … ?



Applications

Cloud Computing Layer

Webbrowser

Managed Runtime

Operating System

Virtual Machine

Hardware

Is Virtual Better Than Real ?

HEISE ...

- 7.11.2008: Bug in VMware's CPU emulation grants elevated privileges
- 31.10.2008: VMware patches ESX server to close security holes
- 6.10.2008: VMware patches various vulnerabilities
- 19.9.2008: security update for VMware ESX

Virtual Machines

- Isolation

- Reuse of COTS Operating Systems and Applications
  through (Virtual) Hardware interface

At the price of complexity !

Virtual Machines

- Isolation

Micro Kernels

Virtual
Machine
Monitors

- Reuse of COTS Operating Systems and Applications
through (Virtual) Hardware interface

At the price of complexity !

Micro-Kernels

- Isolation and Communication
- Highly Efficient IPC
- IPC Control through Capability System
- Security Policy through IPC Control

- Operating Systems Based on Small, Isolated, Securely Interacting Components

Orthogonal and complementary technologies

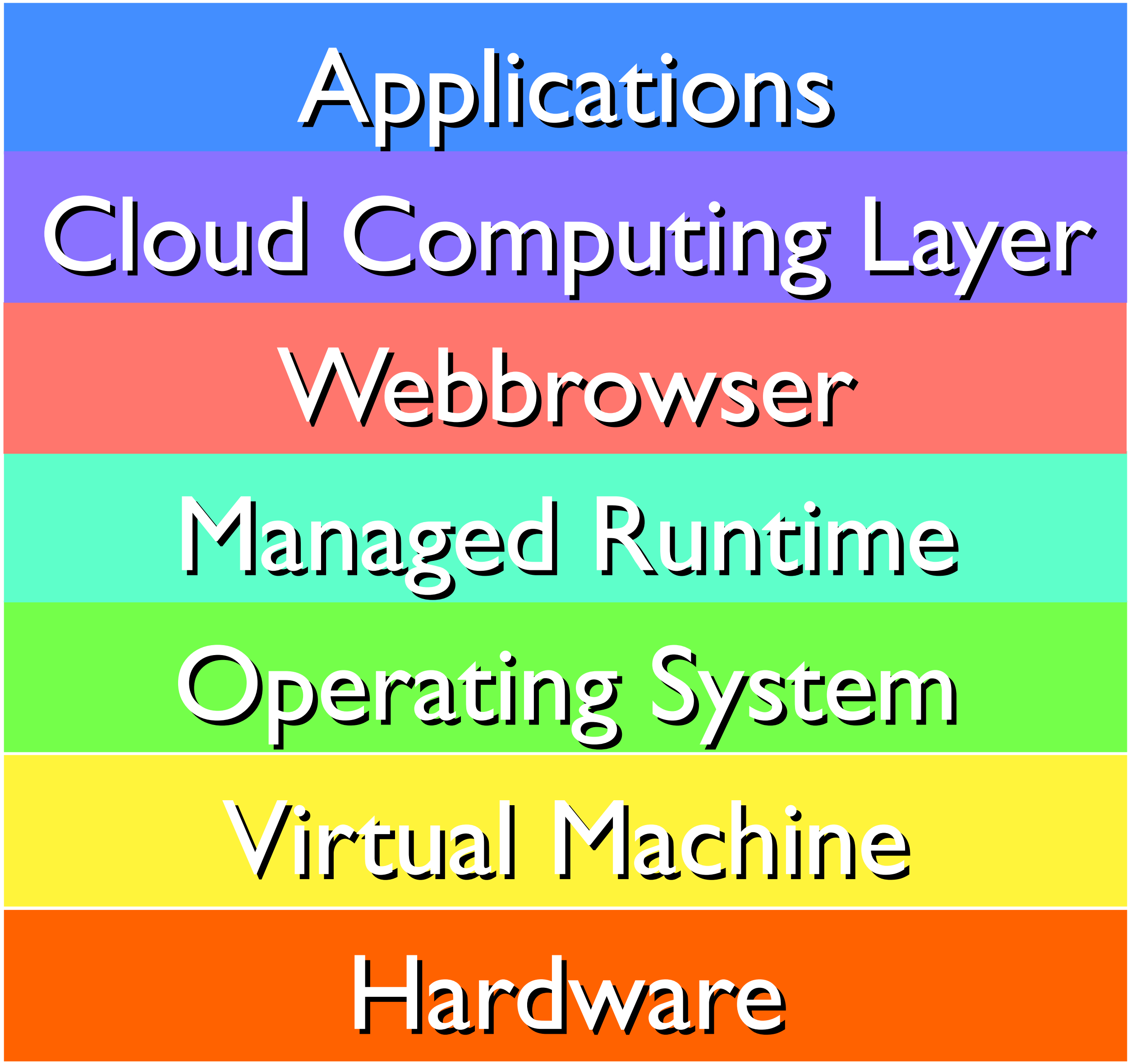
- Micro-kernels → Isolation
- Virtual Machines → (Virtual) HW Interface

Light-Weight Micro-Kernels

- Componentisation of Operating Systems
- Split applications, run critical on Micro-Kernel, uncritical on COTS Operating Systems

Small Trusted Computing Bases

Any Better ... ?



Applications

Cloud Computing Layer

Webbrowser

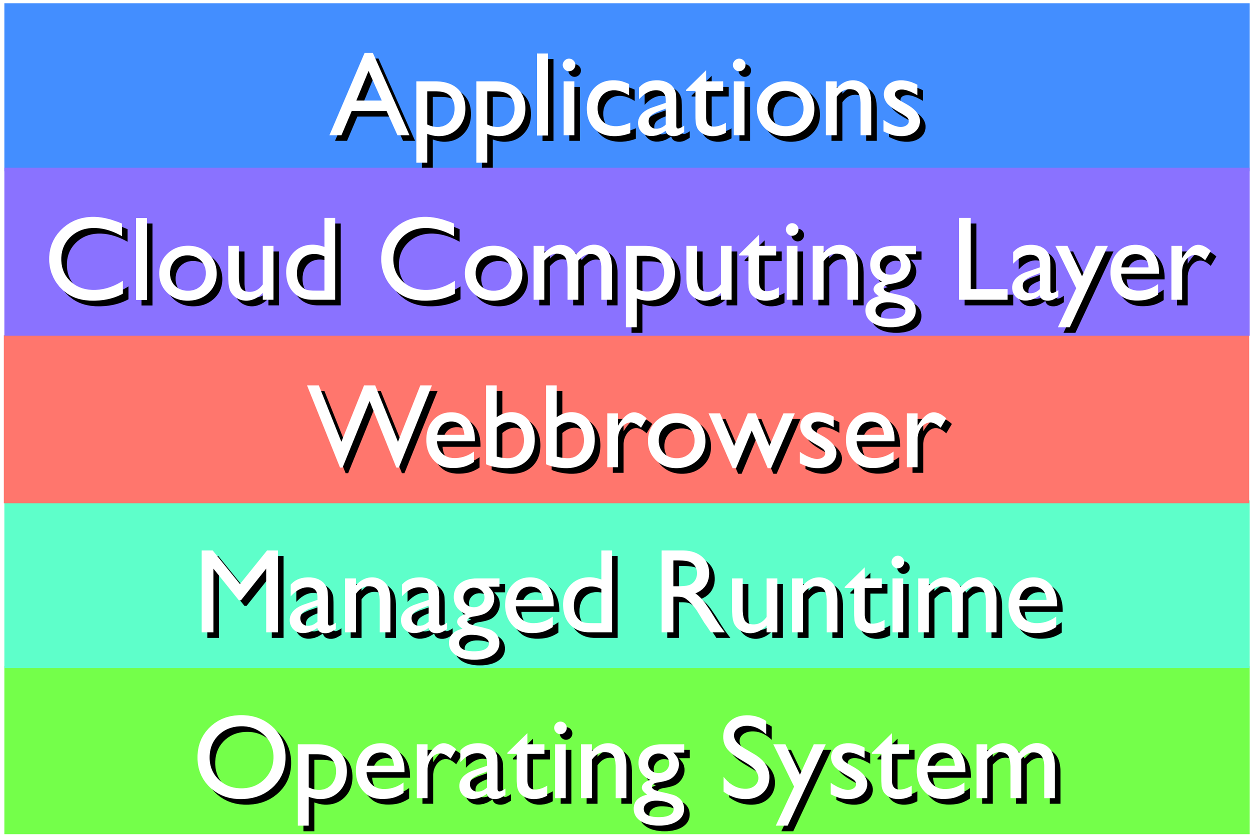
Managed Runtime

Operating System

Virtual Machine

Hardware

Any Better ... ?



Applications

Cloud Computing Layer

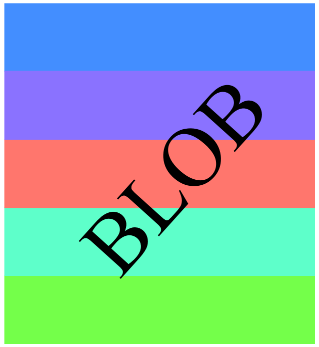
Webbrowser

Managed Runtime

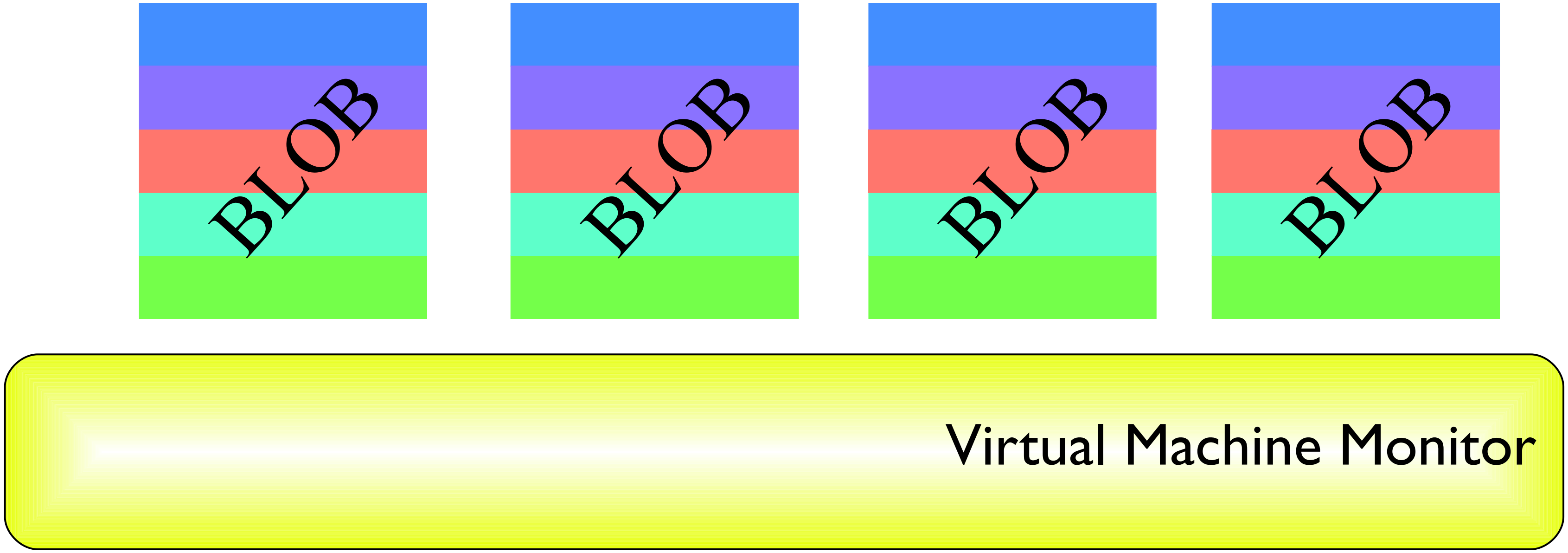
Operating System

Any Better ... ?

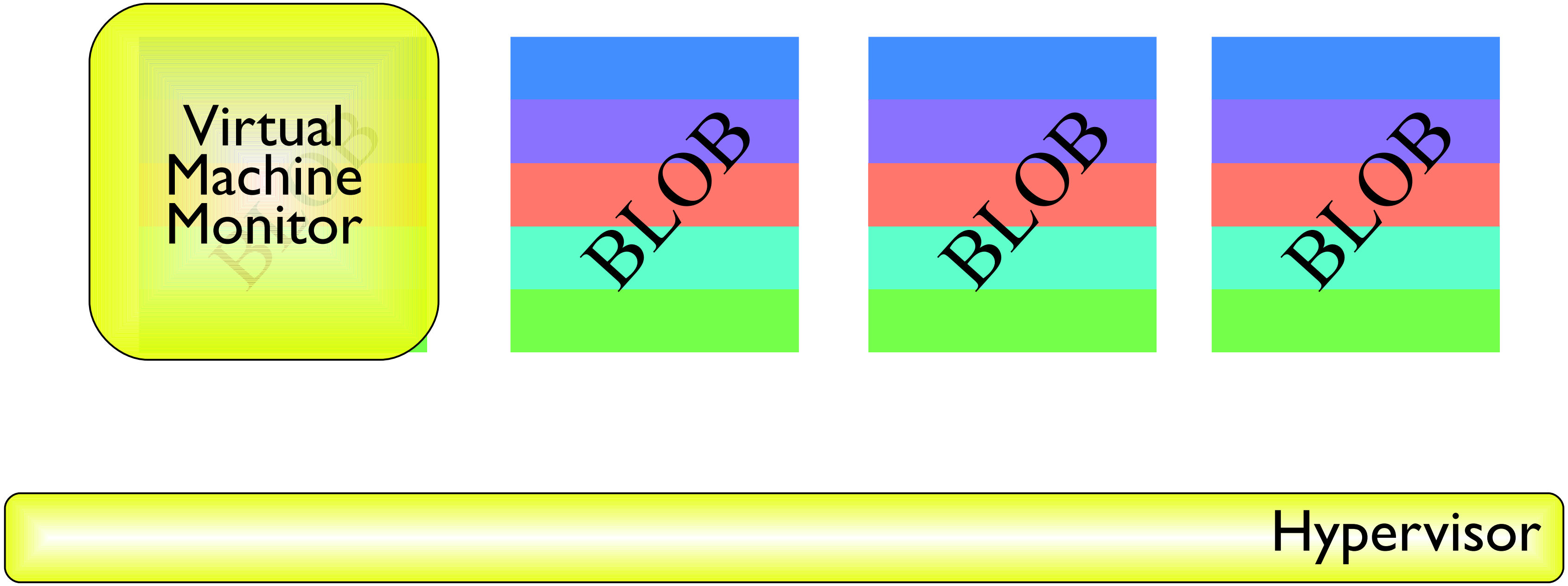
Any Better ... ?



Separate (Virtual) Machines



Smaller Hypervisors



Virtual Machine Monitor

BLOB

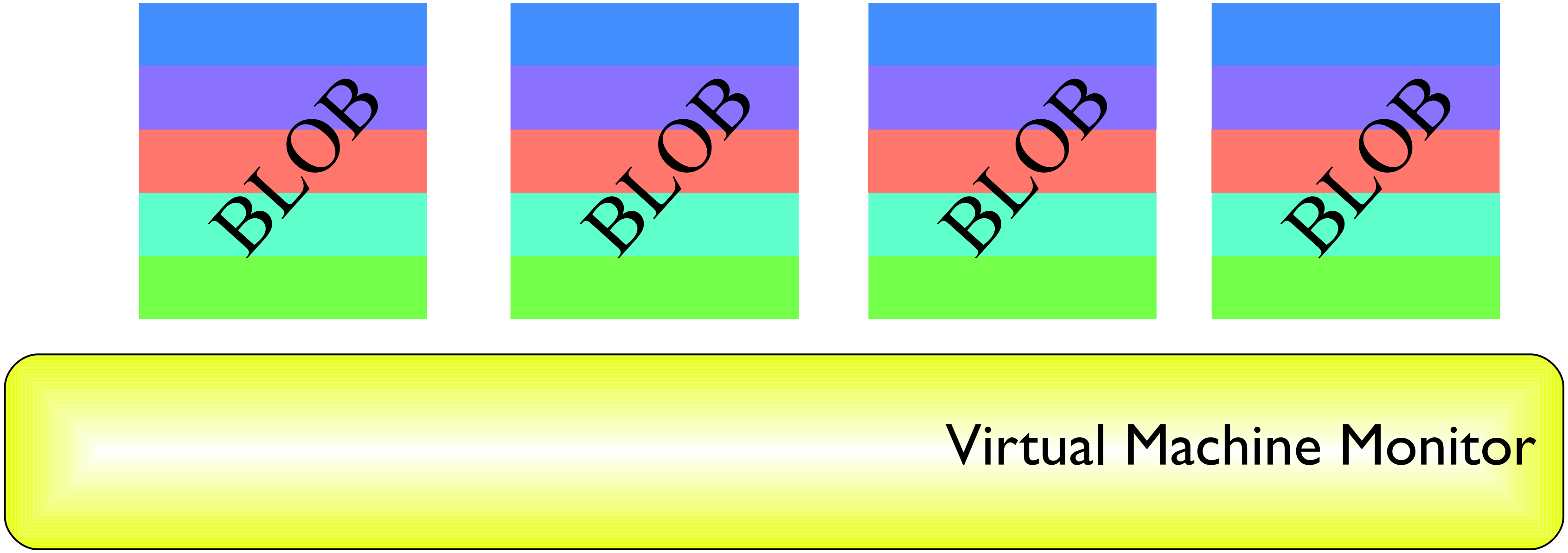
BLOB

BLOB

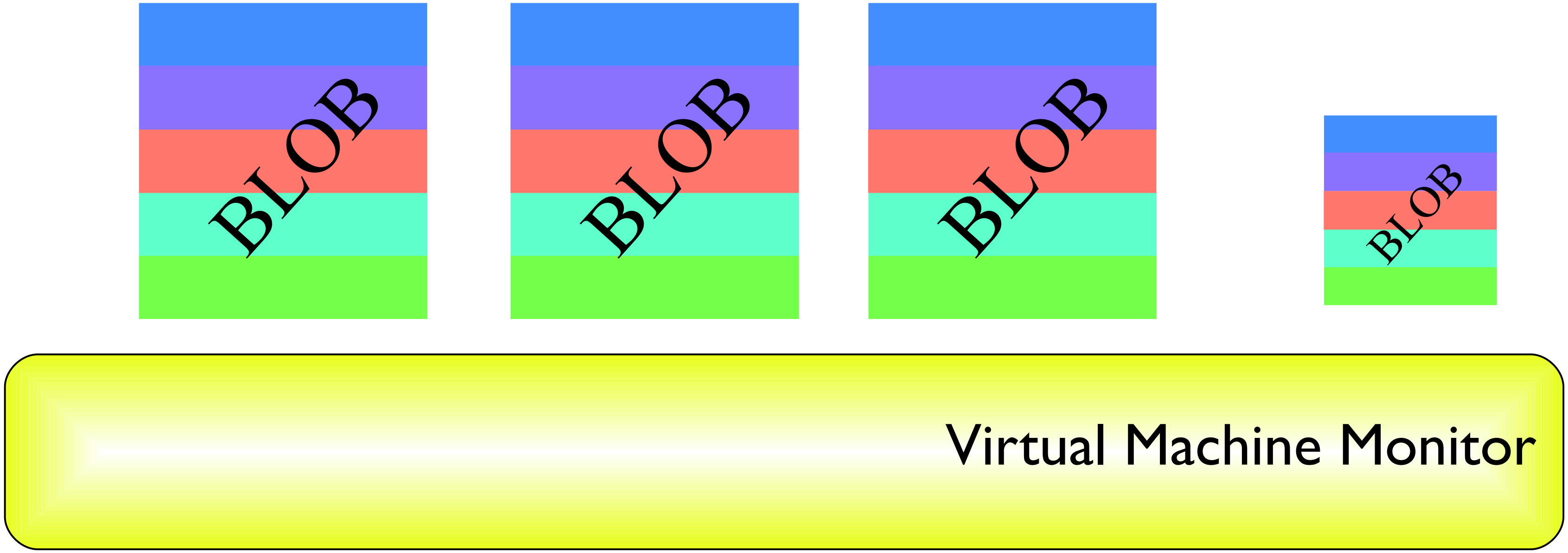
BLOB

Hypervisor

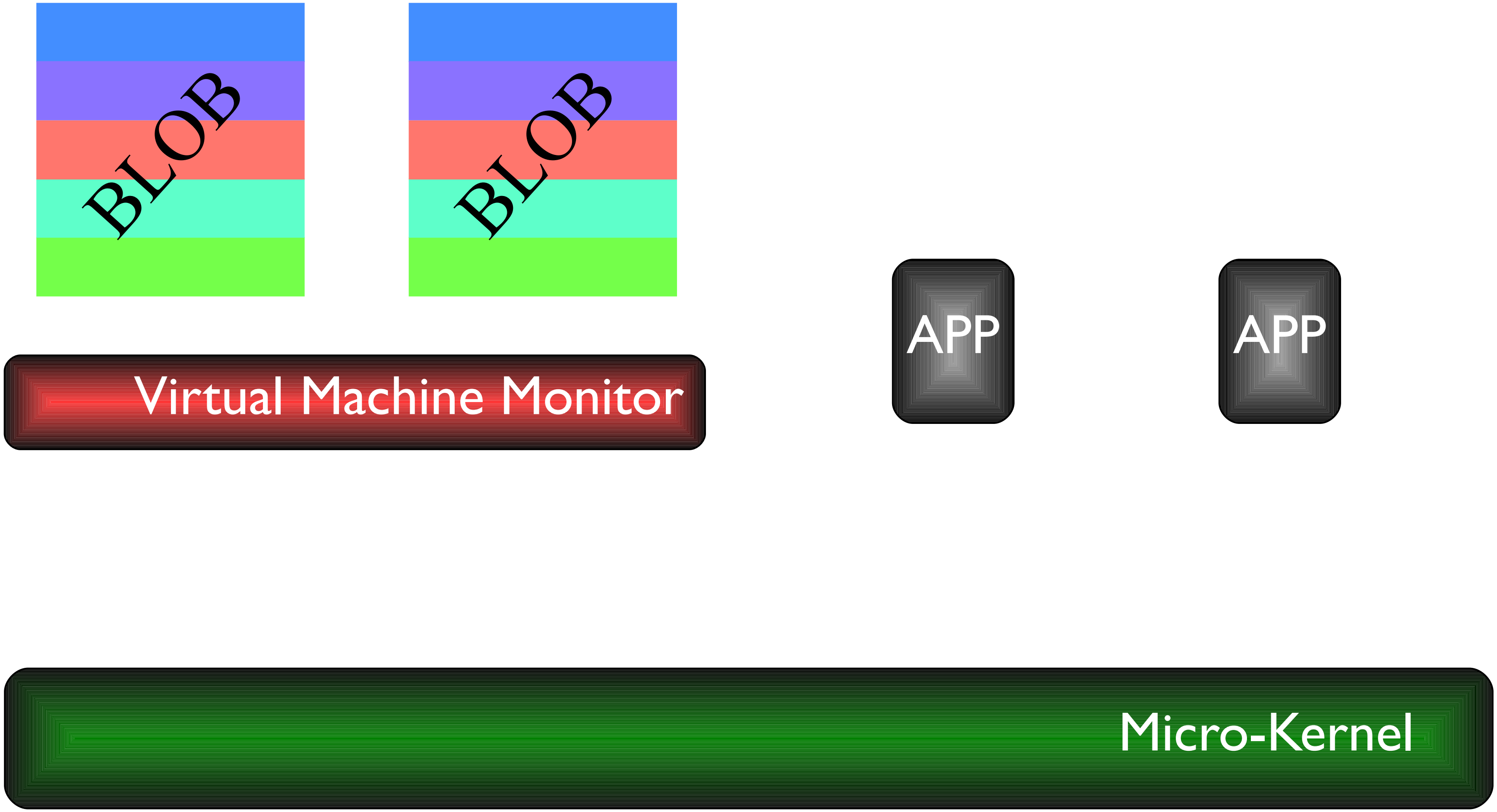
Separate (Virtual) Machines



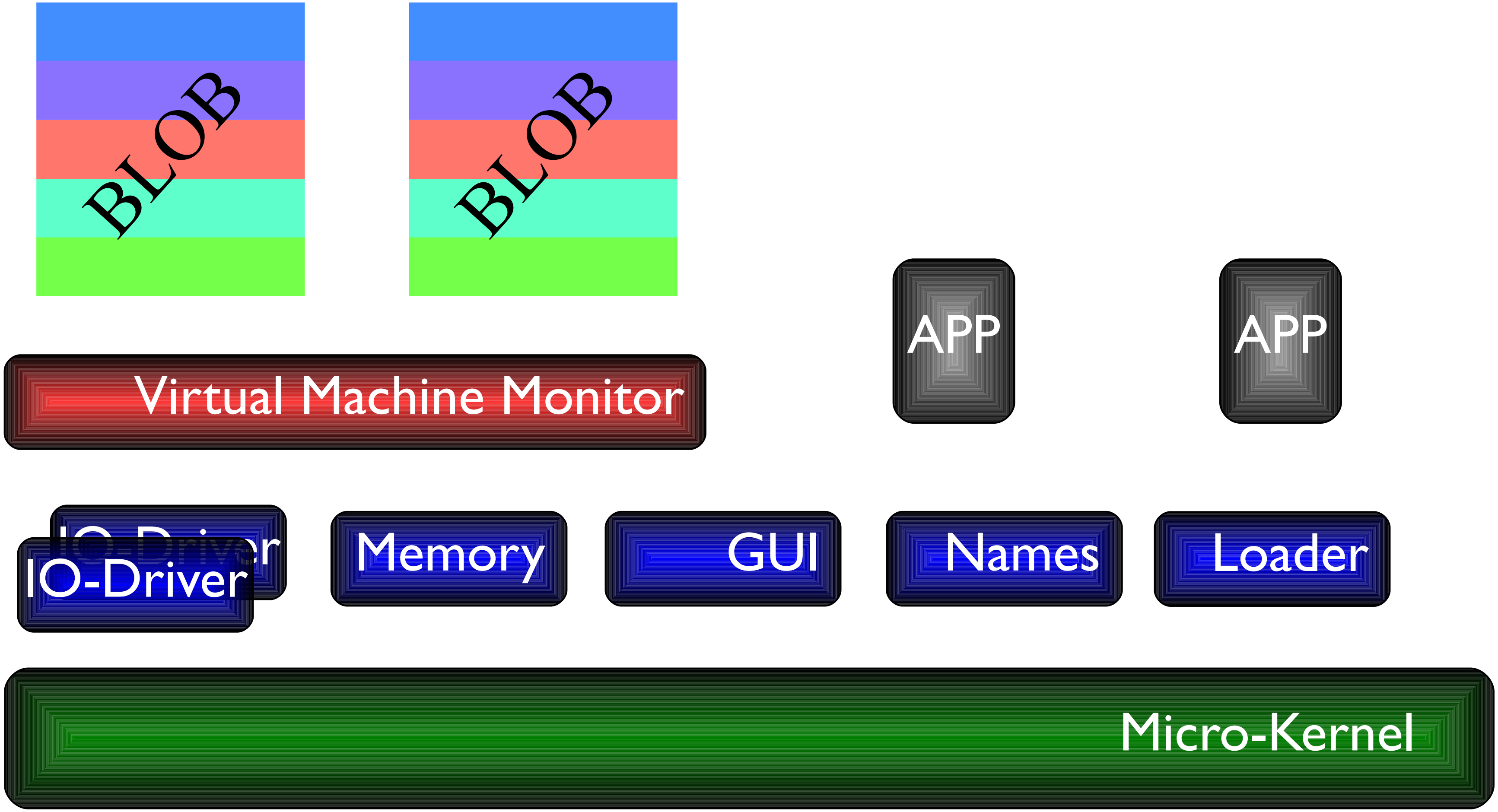
Smaller, Special Purpose BLOBs



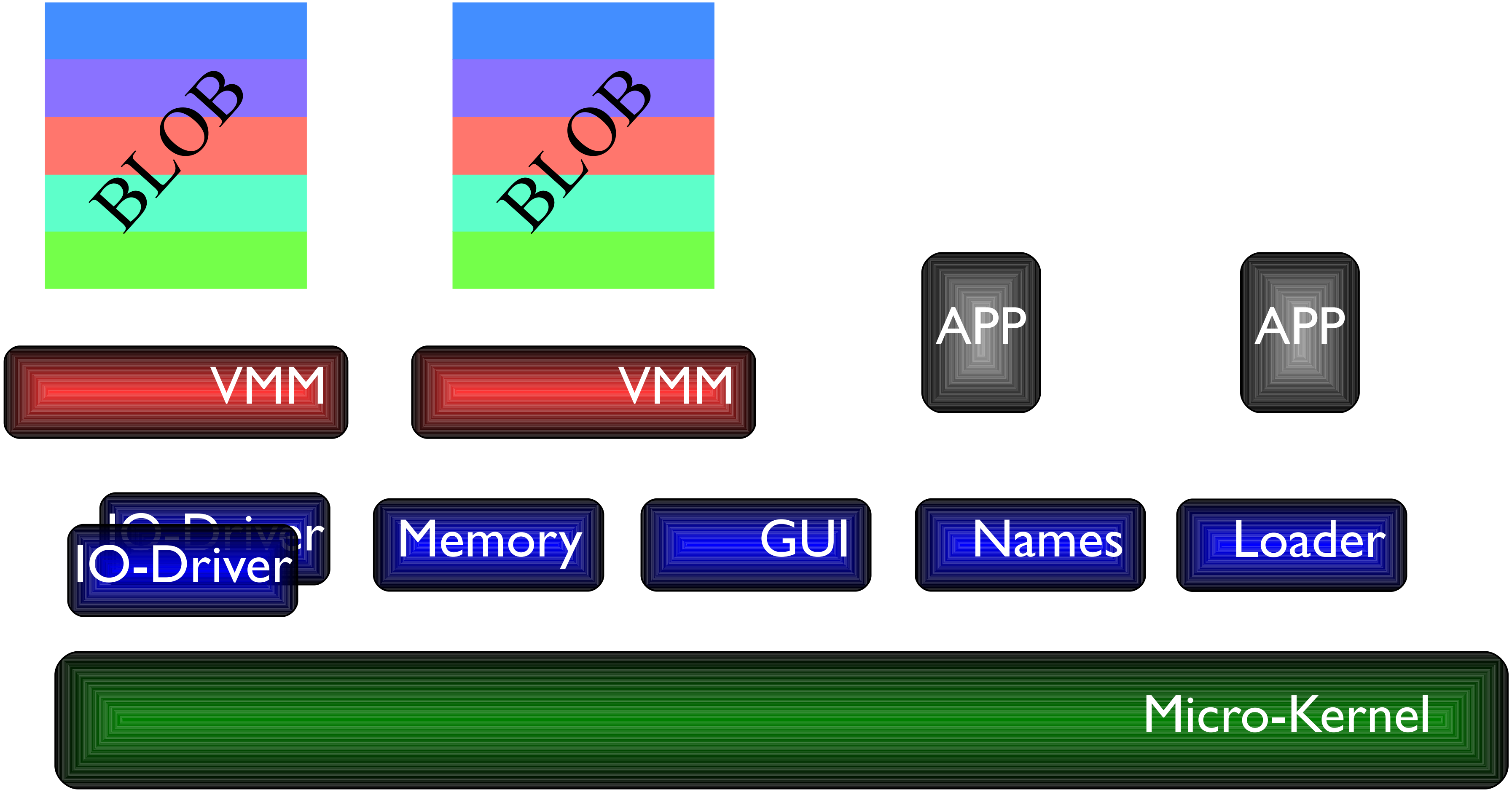
BLOBs/VMs plus Critical Applications ...



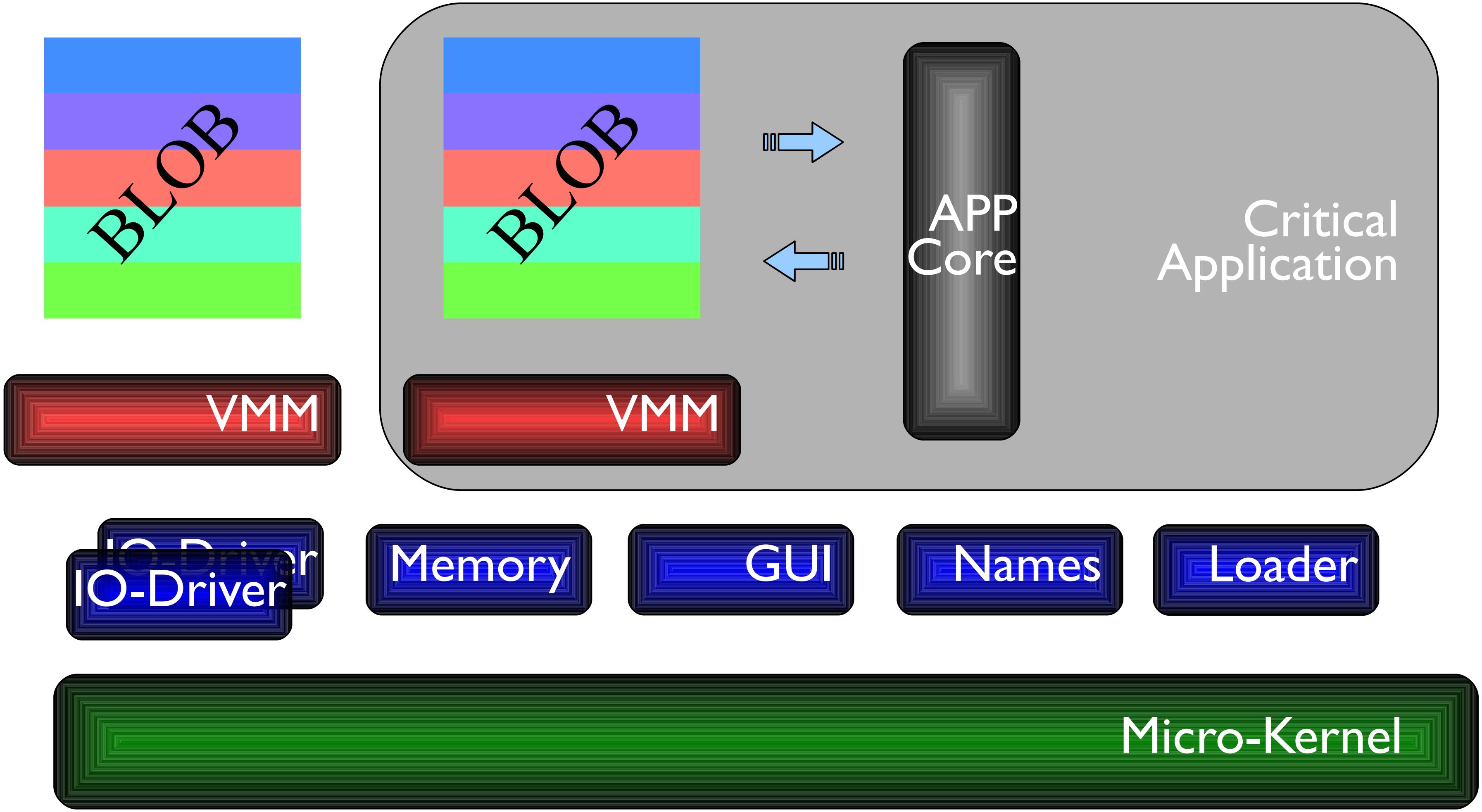
… Based on Componentised, Small OS

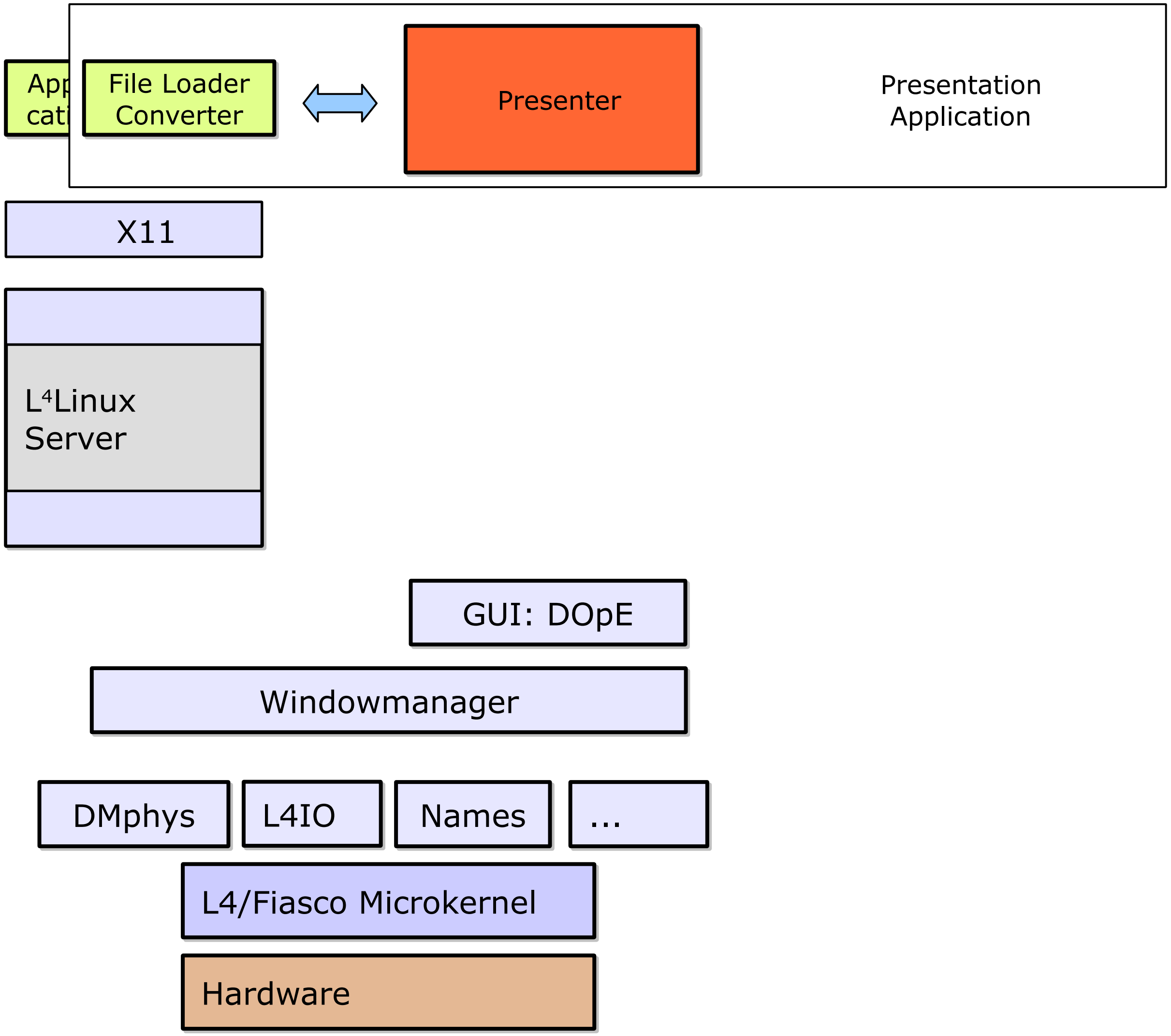


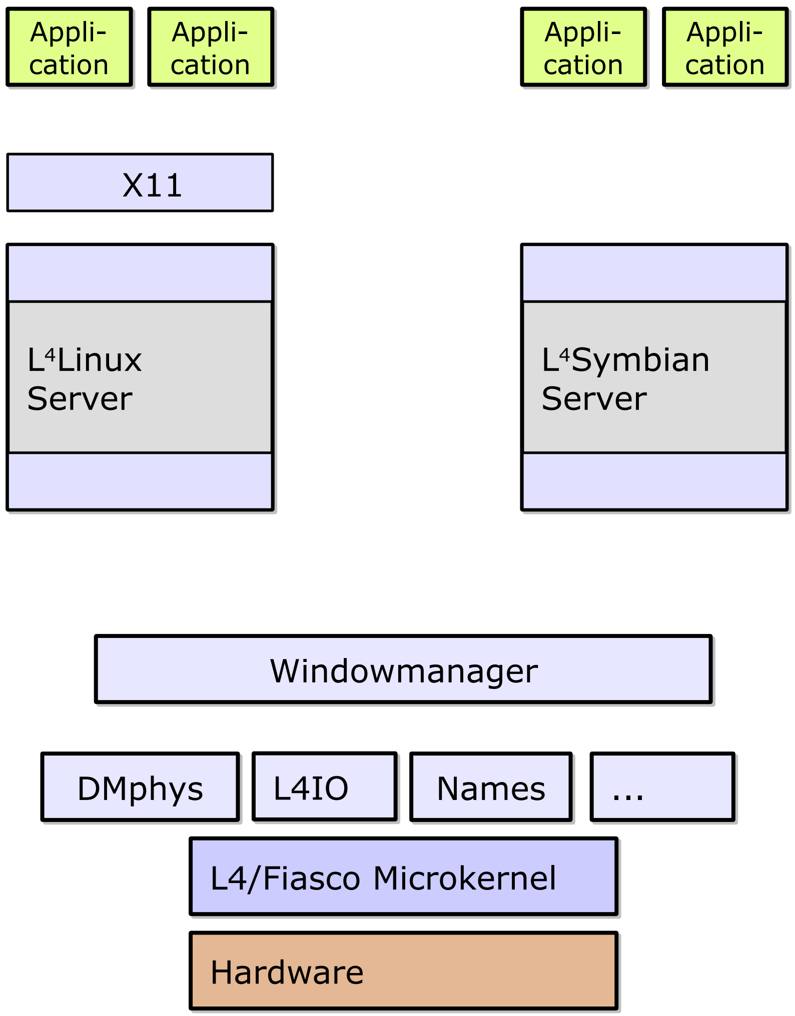
Separate Virtual Machine Monitors?



Reuse COTS for Critical Applications



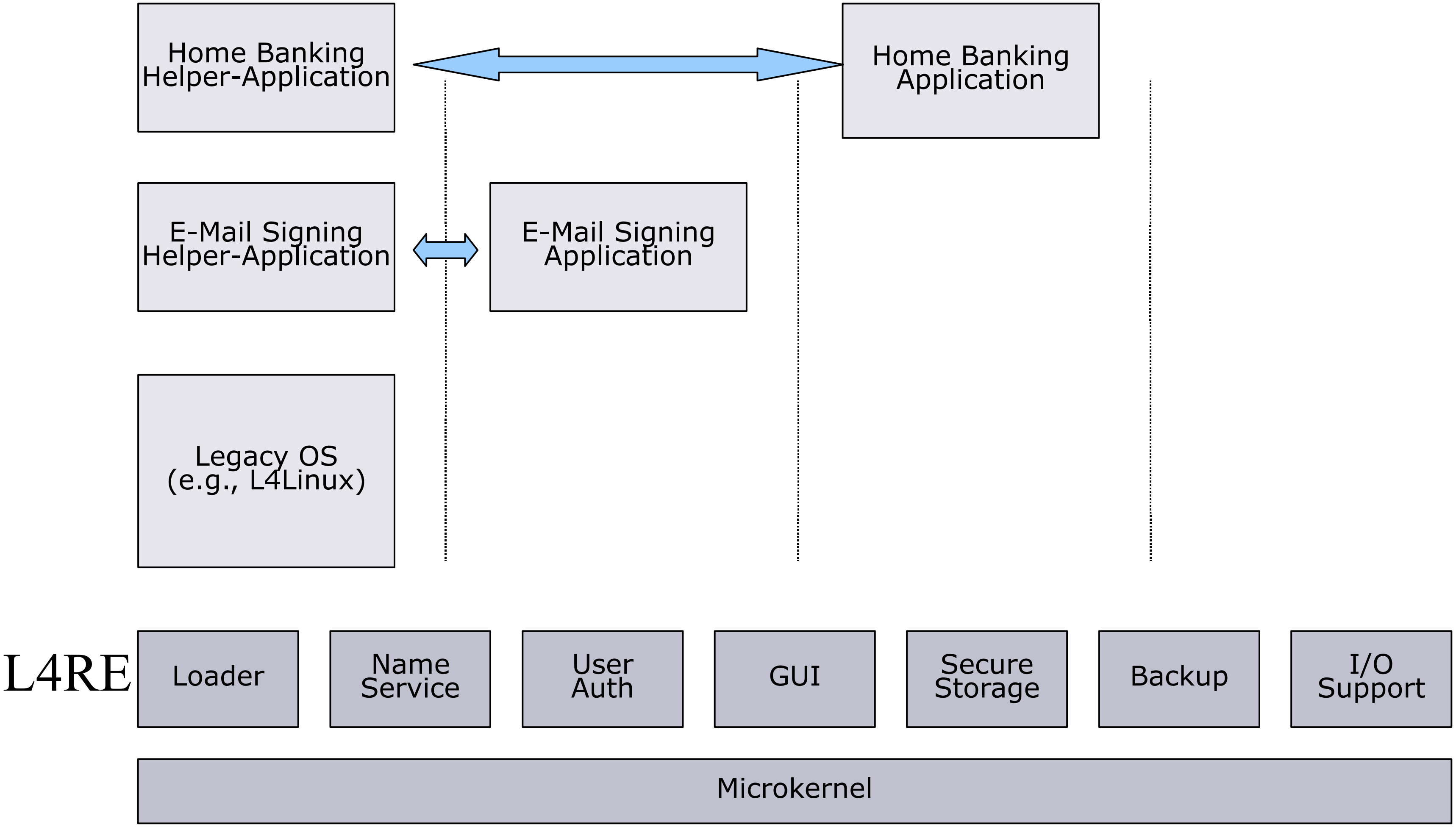

App
cati
File Loader
Converter
Presenter
Presentation
Application
X11
L4Linux
Server
GUI: DOpE
Windowmanager
DMphys
L4IO
Names
...
L4/Fiasco Microkernel
Hardware



“L4RE”

Resource Management and Virtualization Support Layer

L4/Nizza Architecture



Home Banking Helper-Application

Home Banking Application

E-Mail Signing Helper-Application

E-Mail Signing Application

Legacy OS (e.g., L4Linux)

L4RE

Loader

Name Service

User Auth

GUI

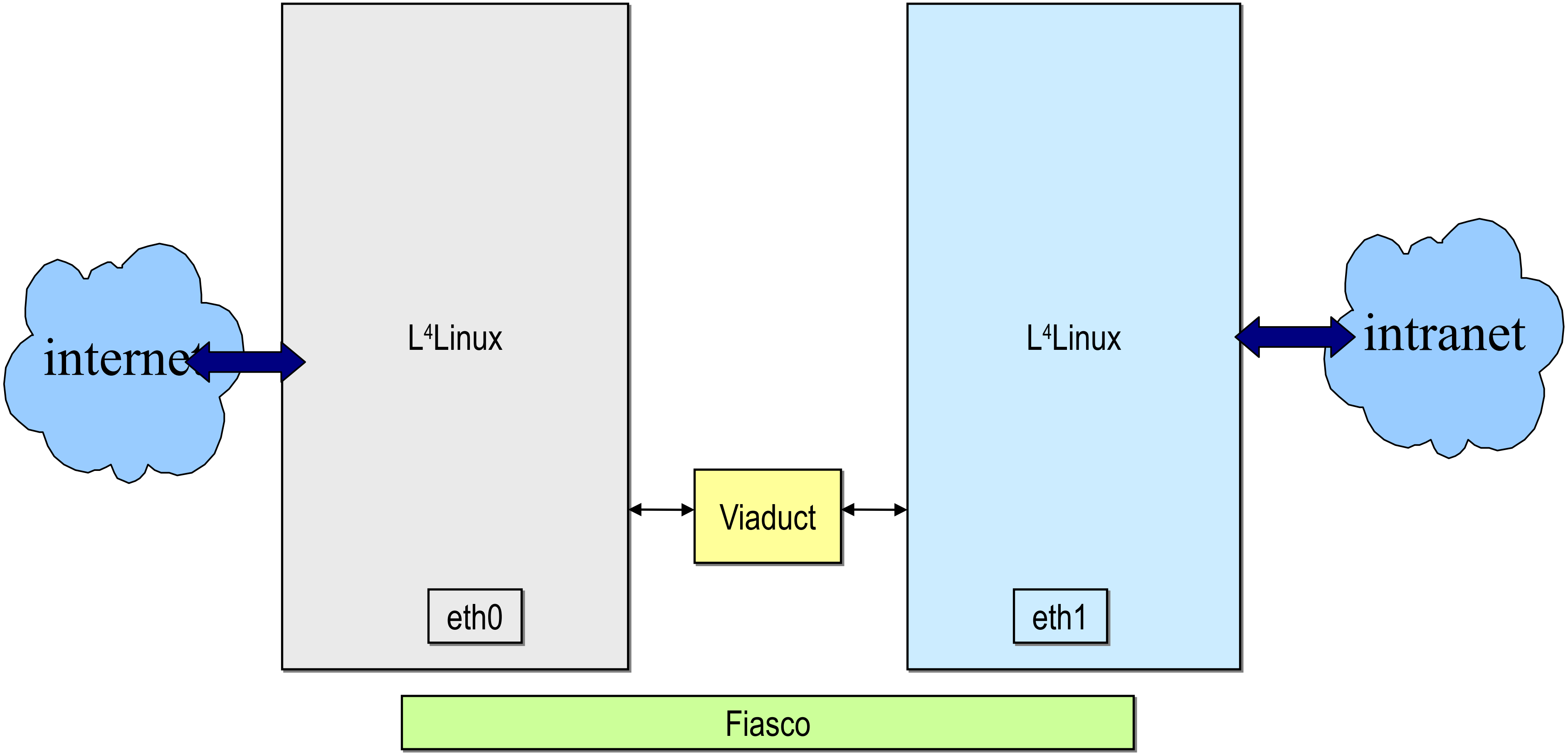
Secure Storage

Backup

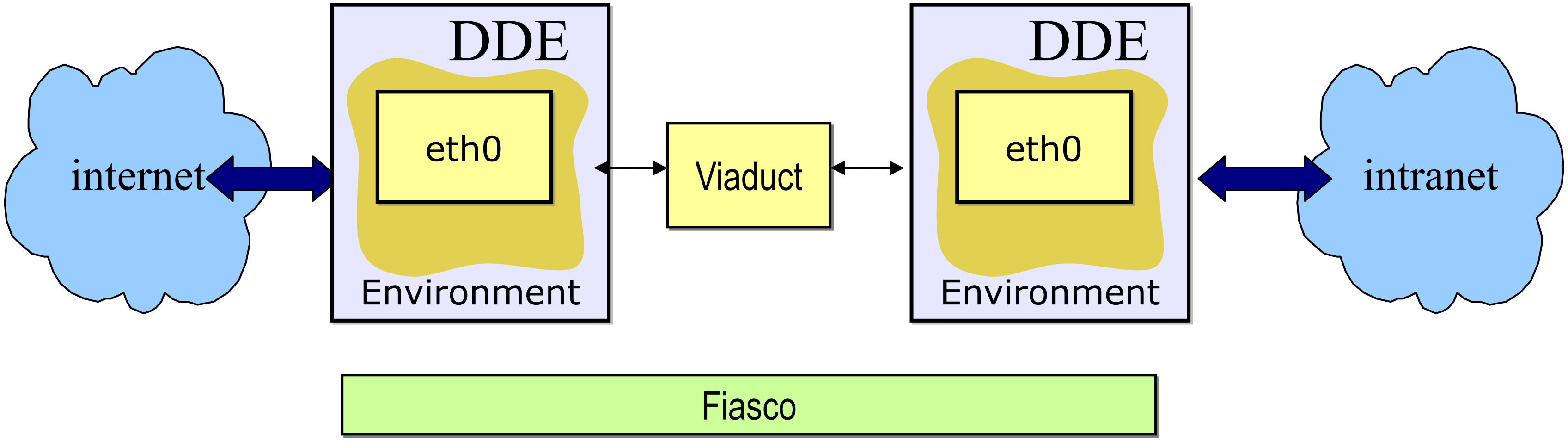
I/O Support

Microkernel

L4/Nizza Applications: VPN

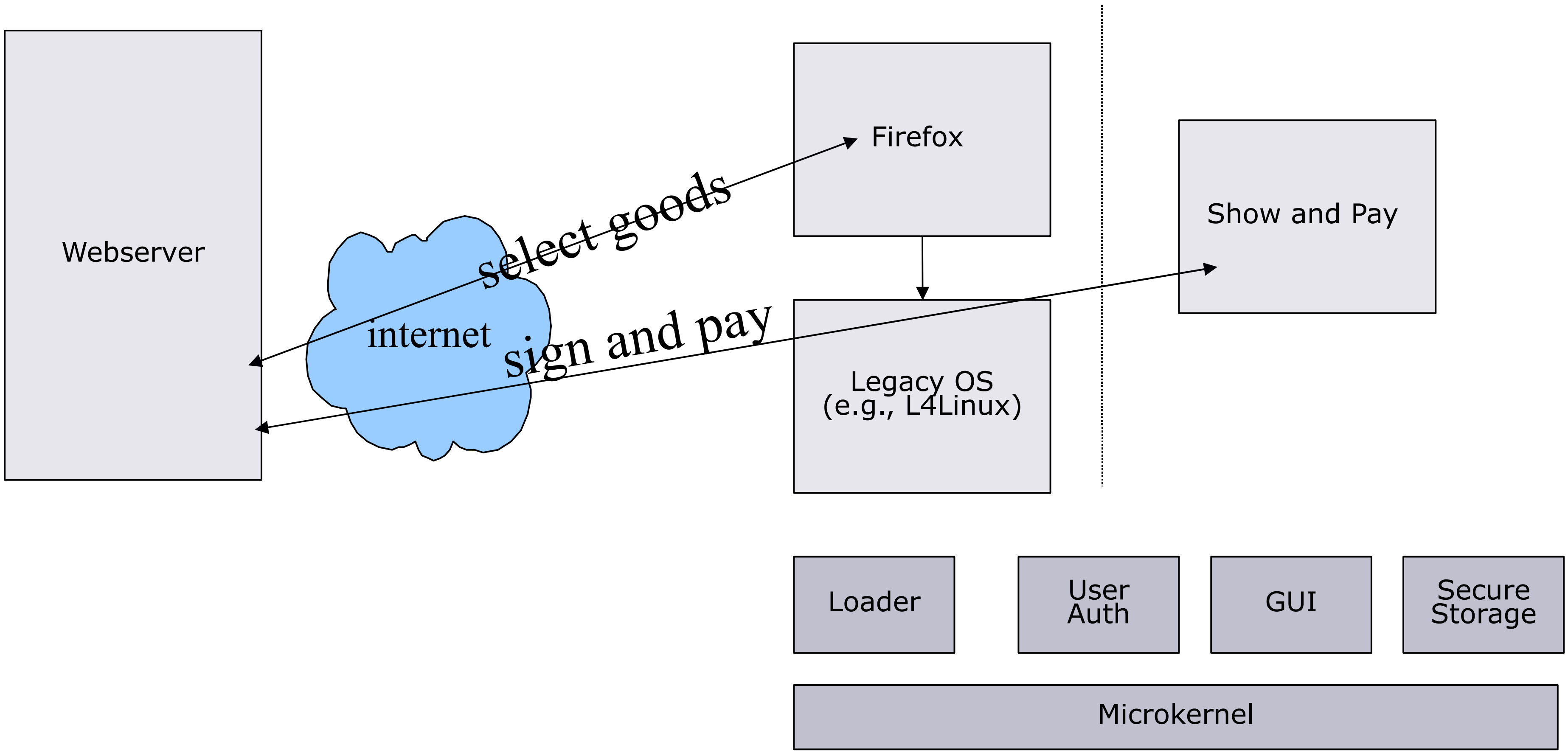


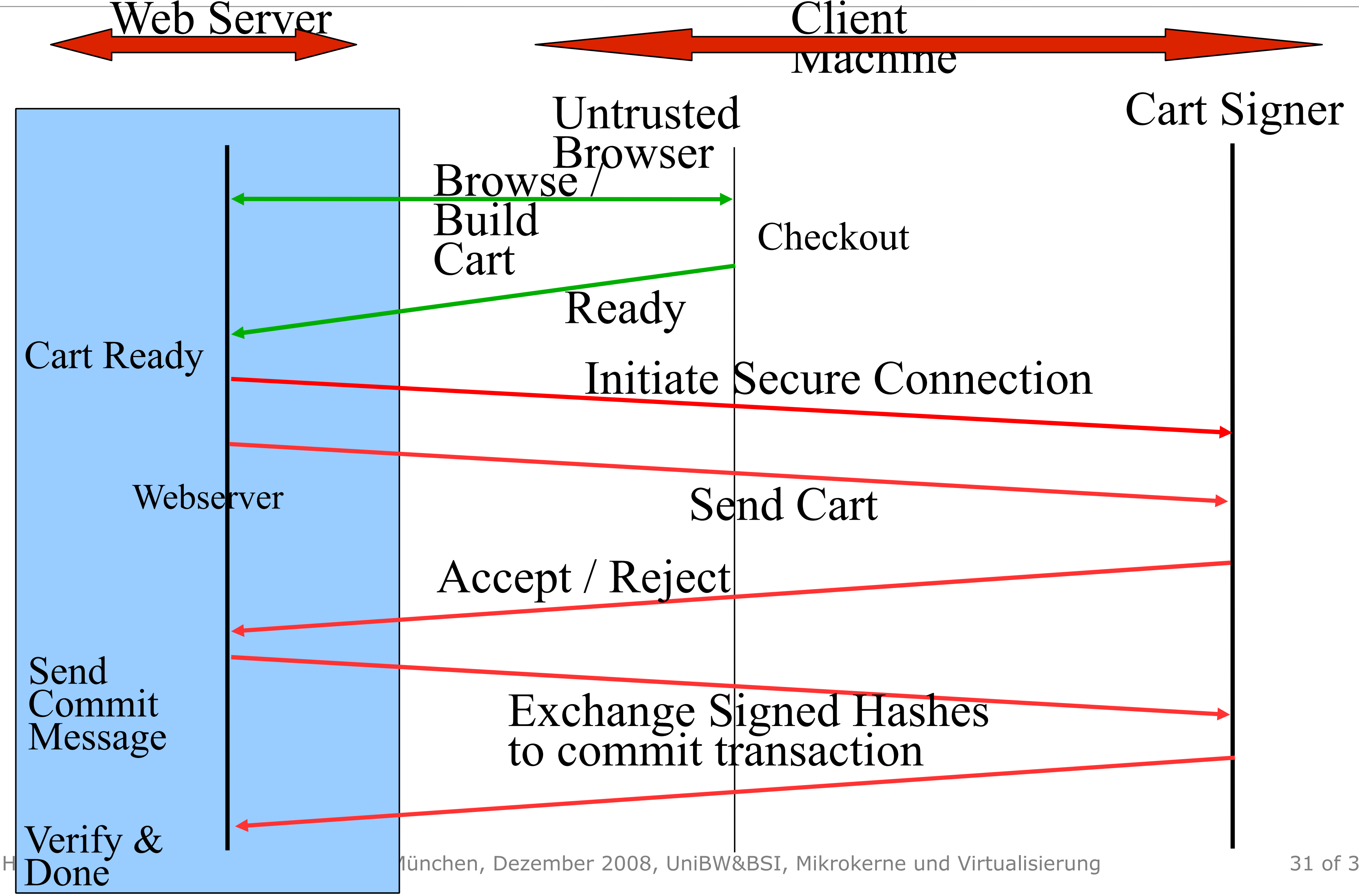
L4/Nizza Applications: VPN



L4/Nizza Apps: Internet Transaction

…





Web Server

Client Machine

Untrusted Browser

Cart Signer

Browse / Build Cart

Checkout

Ready

Cart Ready

Initiate Secure Connection

Webserver

Send Cart

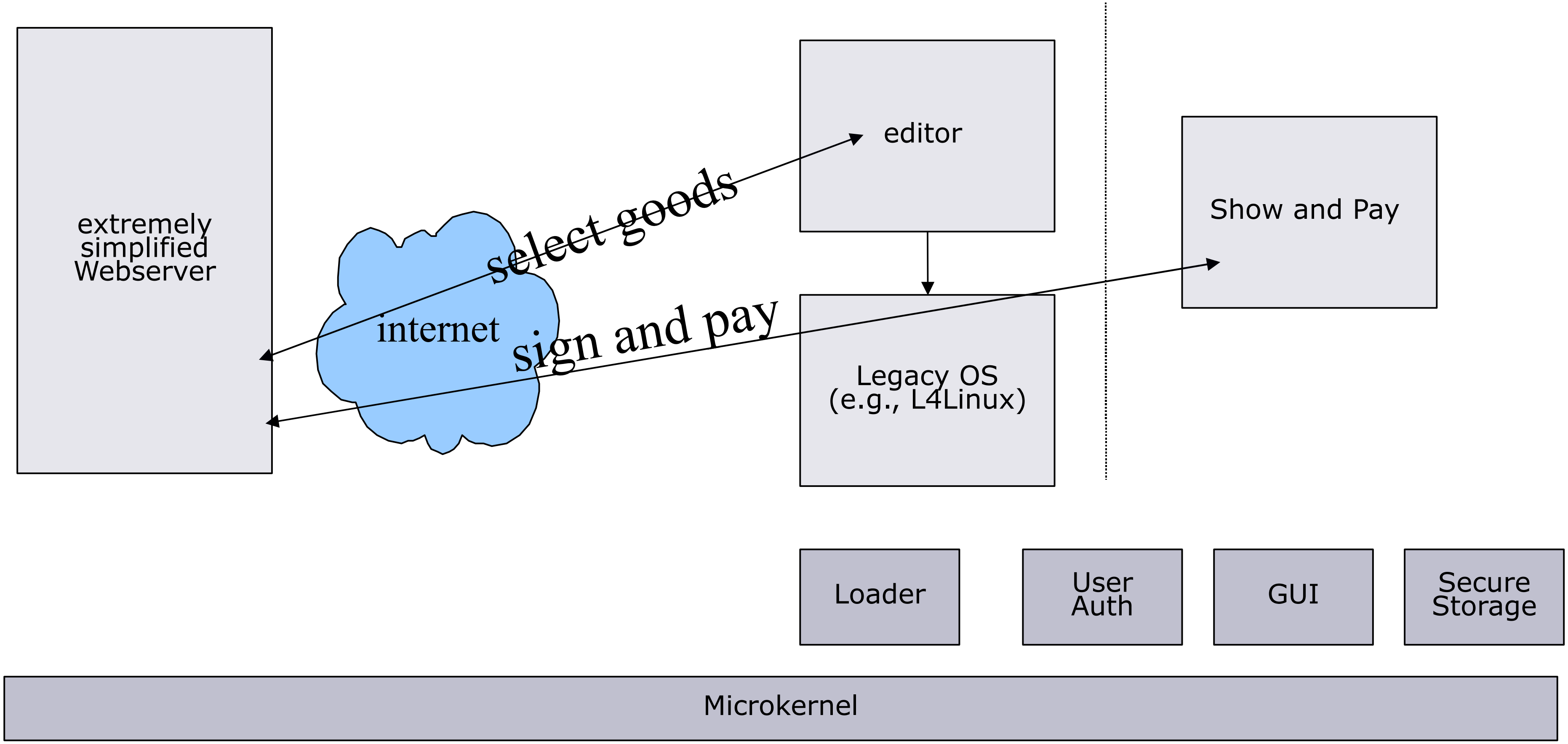
Accept / Reject

Send Commit Message

Exchange Signed Hashes
to commit transaction

Verify & Done

L4/Nizza Apps: Internet Transaction



Complexity Numbers

Scenario	Original Application		AppCore		Reduction Factor
e-commerce (Browser)	978	151	10	1.5	100X
VPN Gateway (FreeS/WAN)	155	25	74	10	2.1X
Email signer (Thunderbird)	250	45	54	11	4.6X
TCB (Linux+Xserver)	1,485	238	100	14	14X

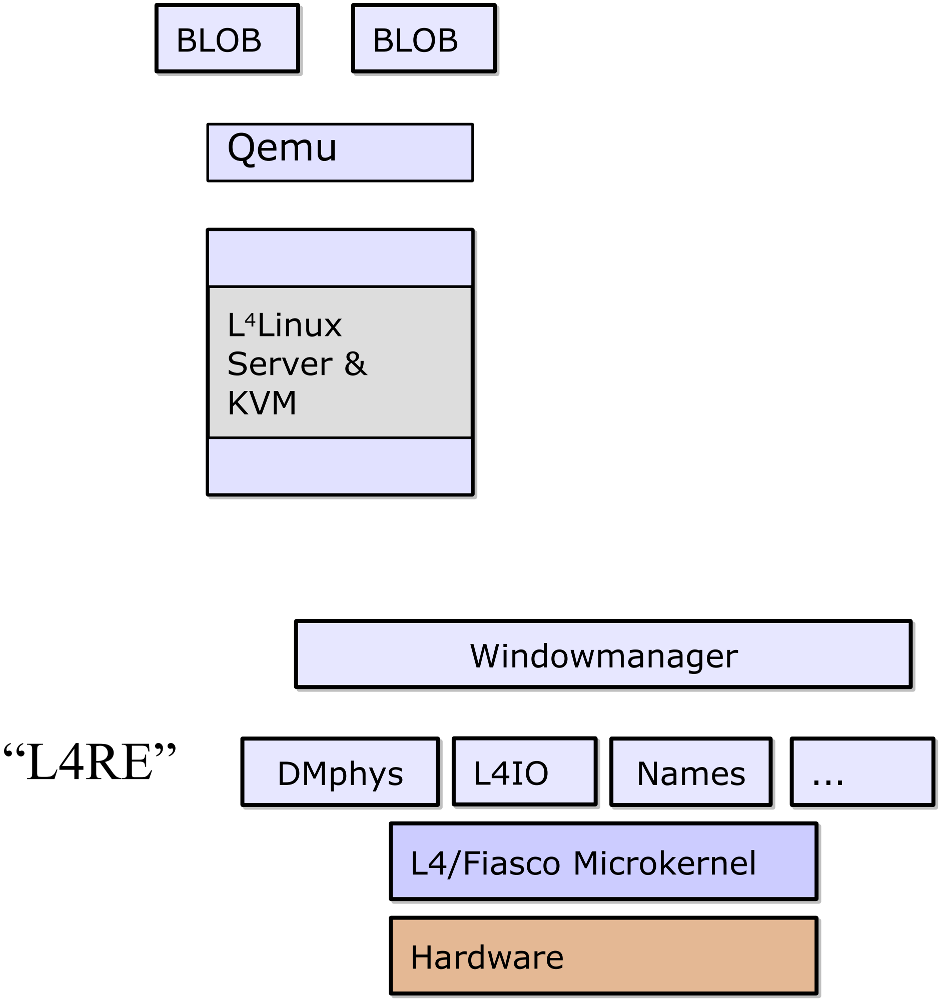
Reducing TCB Complexity for Security-Sensitive Applications: Three Case Studies

Application Possibilities

- Security-Sensitive Applications
- Safety-Critical Scenarios
- Real-Time
- ...
- Combinations thereof

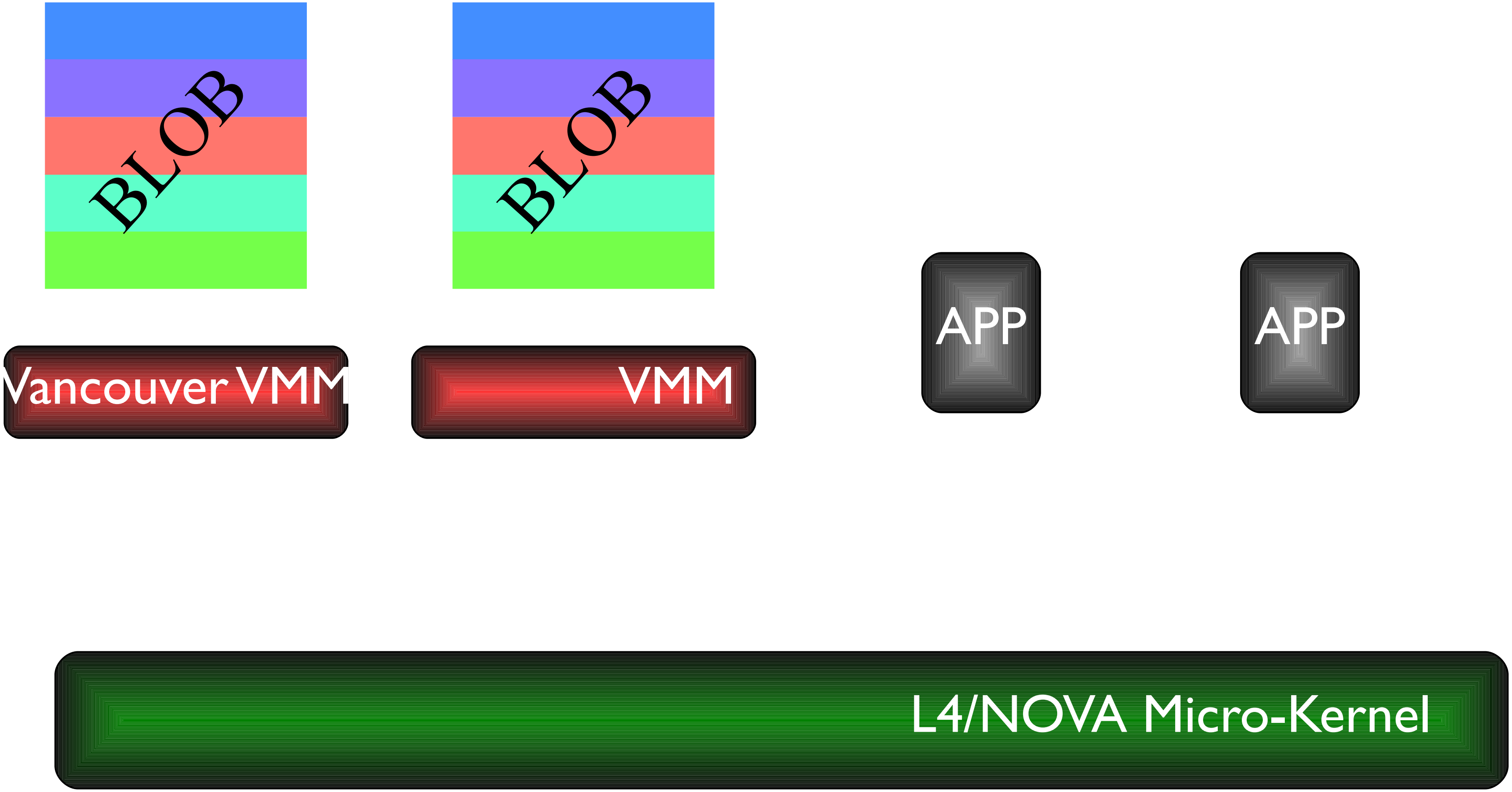
Prototypes in Dresden & San Diego

- Full Virtualisation on KVM/L4Linux/L4Fiasco
- Full Virtualisation with 30KLoC on Vancouver/L4NOVA



Nested Page Tables Required !!!

San Diego OSDI-Poster 12/2008



BLOB

BLOB

Vancouver VMM

VMM

APP

APP

L4/NOVA Micro-Kernel

Research Needs

- Components based on Capability Micro-Kernels
- Split Applications
- Formal Verification
- Applications
  - Safety Critical System
  - More on Security

Conclusions

- Combine COTS and Security-Sensivity
- Reduce Size (and Complexity) by orders of Magnitude
- Support and Reuse Legacy Software
- German Academia are Leading Players