Microkernel Architecture and Security

Advanced Operating Systems | Lea Schmierer

Agenda

1. Introduction
2. Microkernel Architecture
3. Security Aspects of Operating Systems
4. Microkernel Architecture and Security
5. Security Focused Operating Systems
6. Some CVEs
7. Summary

Introduction

Topic and Goal

Exploring the Relationship between Microkernel Architecture and Security

Goal:

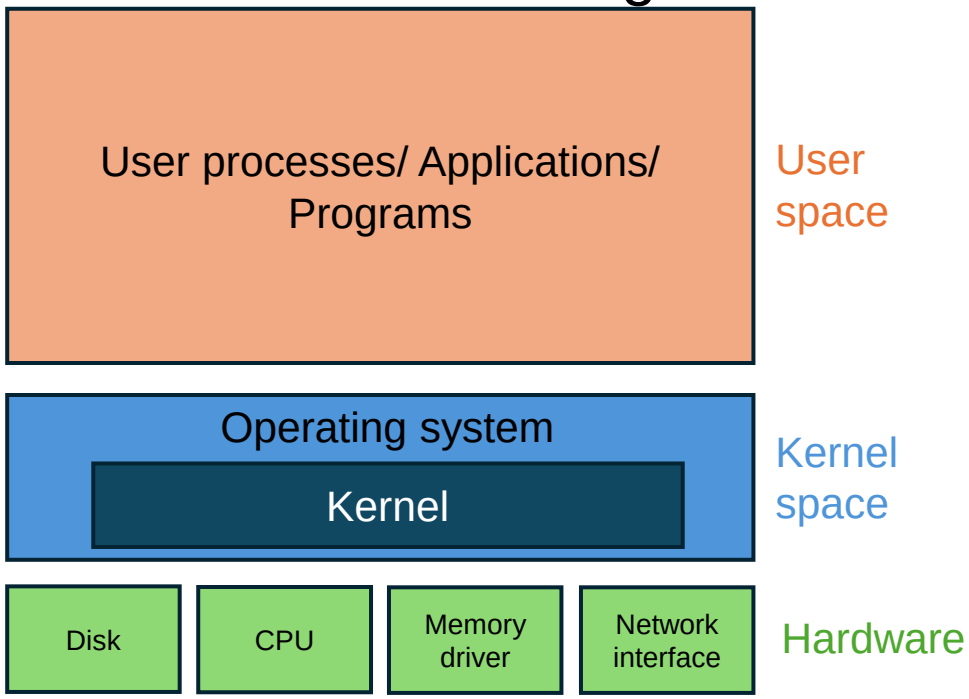
- Overview of fundamental security guarantees
- Discuss additional security considerations

Kernel

- Core component of an OS
- Manages system resources
- Bridges hardware and software interaction

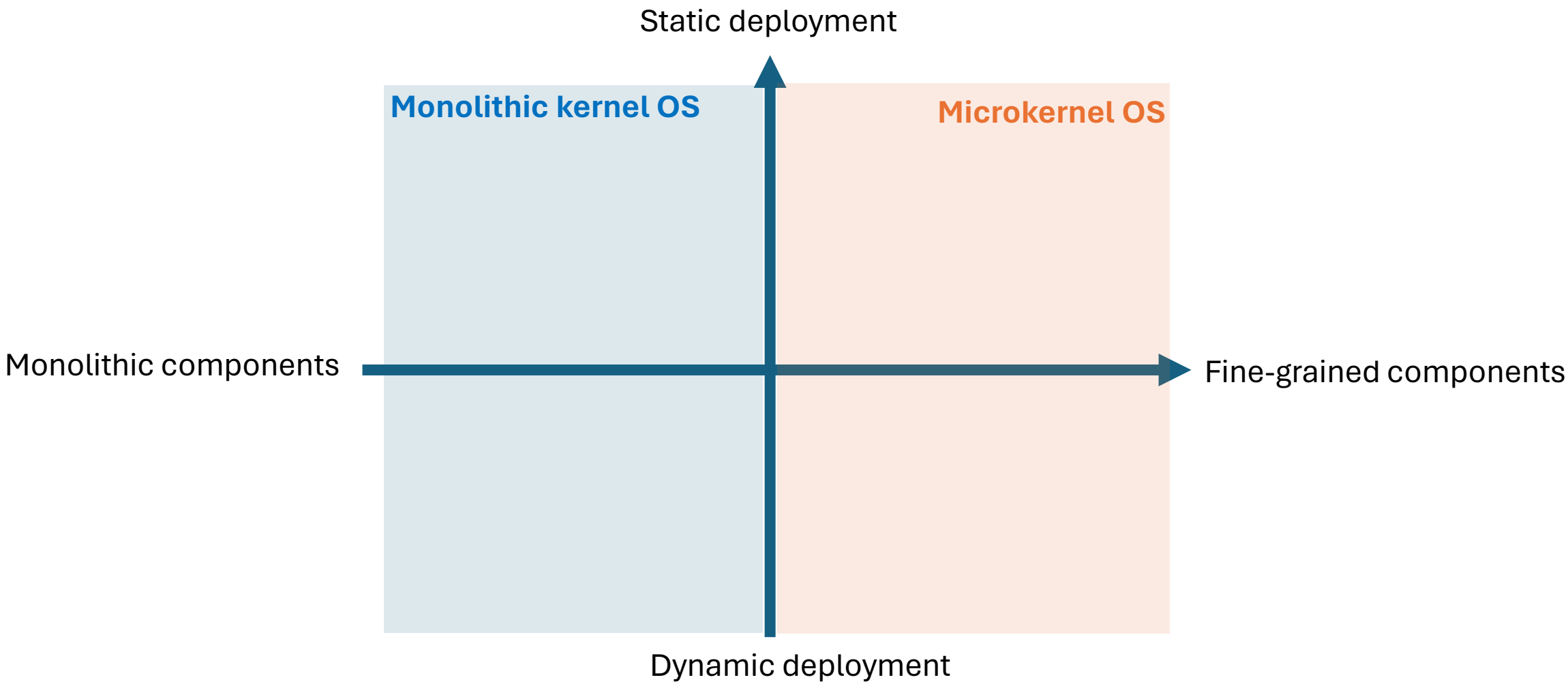
- Kernel design categories:
  - Monolithic kernels
  - Microkernels
  - Hybrid kernels

Monolithic kernel design:



Source: https://medium.com/

Kernel



Source: Martin Děcký, *Microkernel-based and Capability-based Operating Systems*

Microkernel Architecture

Basic Principles

Split of mechanism and policy

Kernel contains just the basic and fundamental mechanisms

Component-based

System composed of isolated components

Separation of concerns

Each component focuses on a well-defined functionality

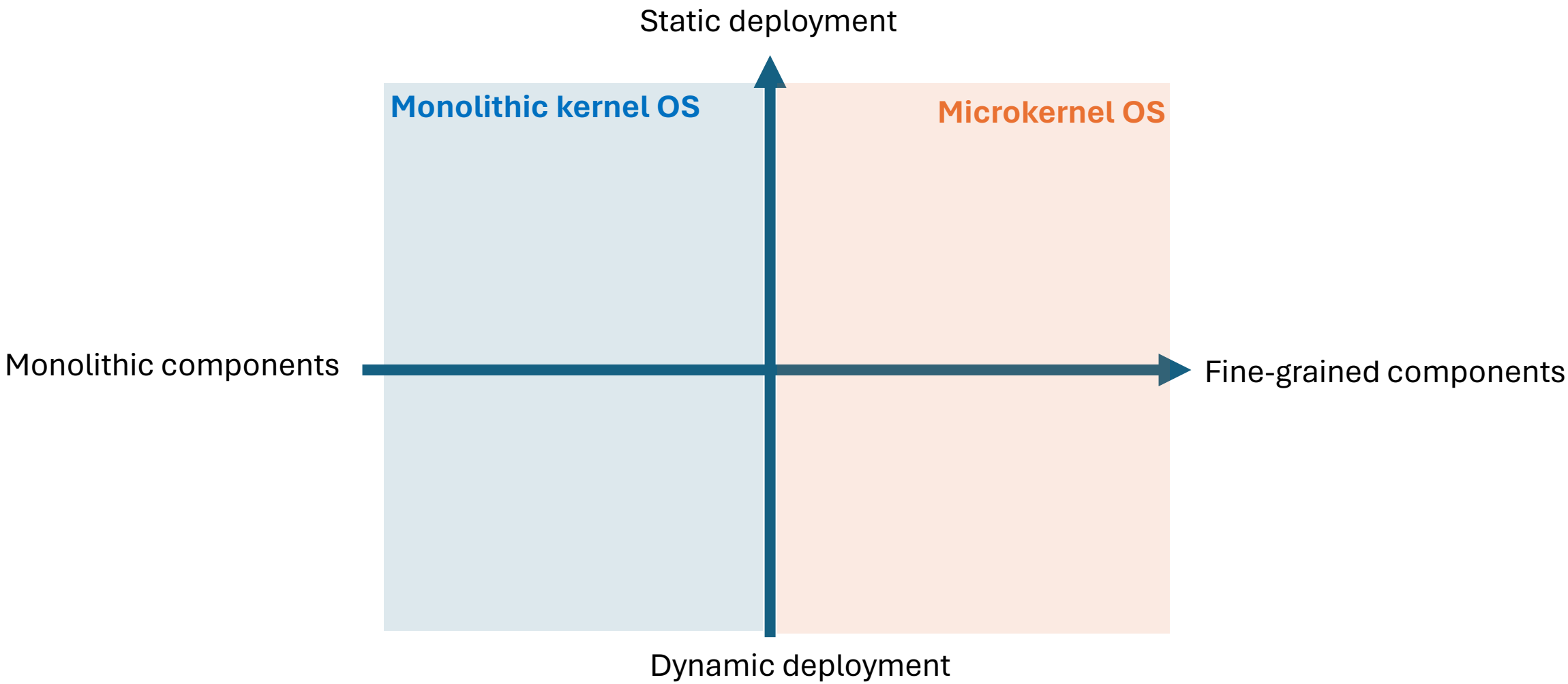
Least privilege

Components have minimal privileges

Modularity

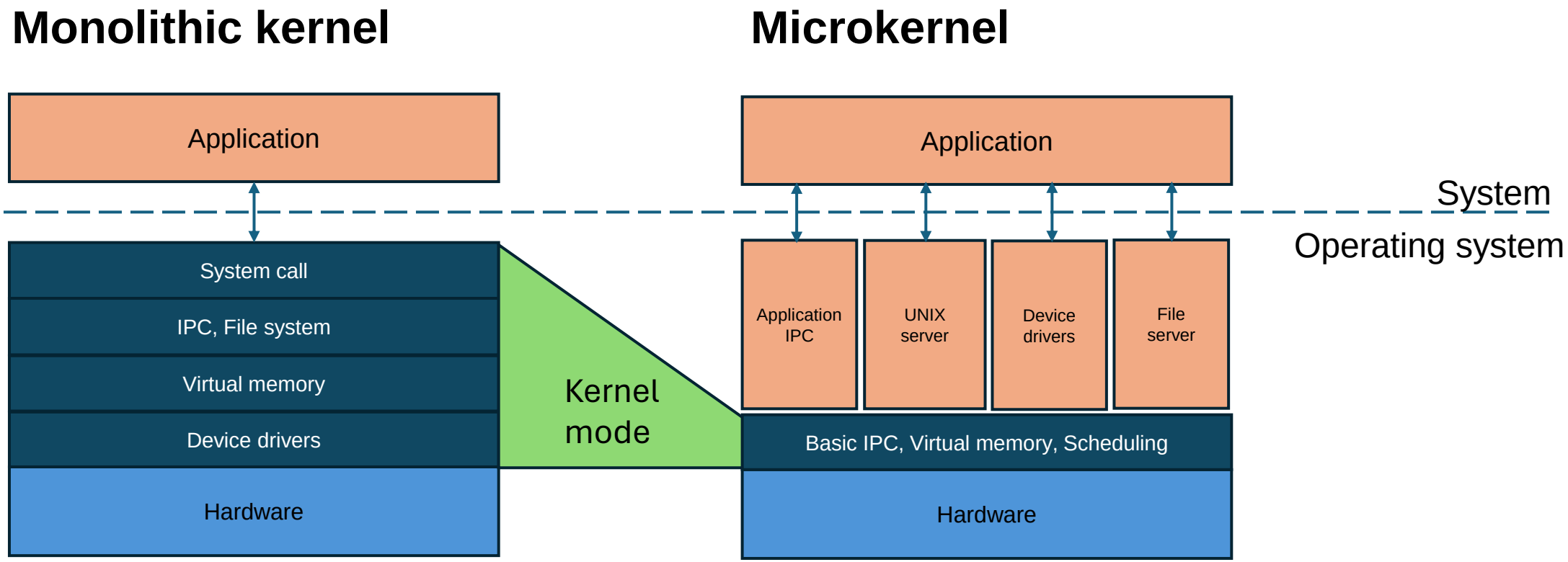
Replacing component implementations

Monolithic Kernel vs. Microkernel



Source: Martin Děcký, *Microkernel-based and Capability-based Operating Systems*

Monolithic Kernel vs. Microkernel

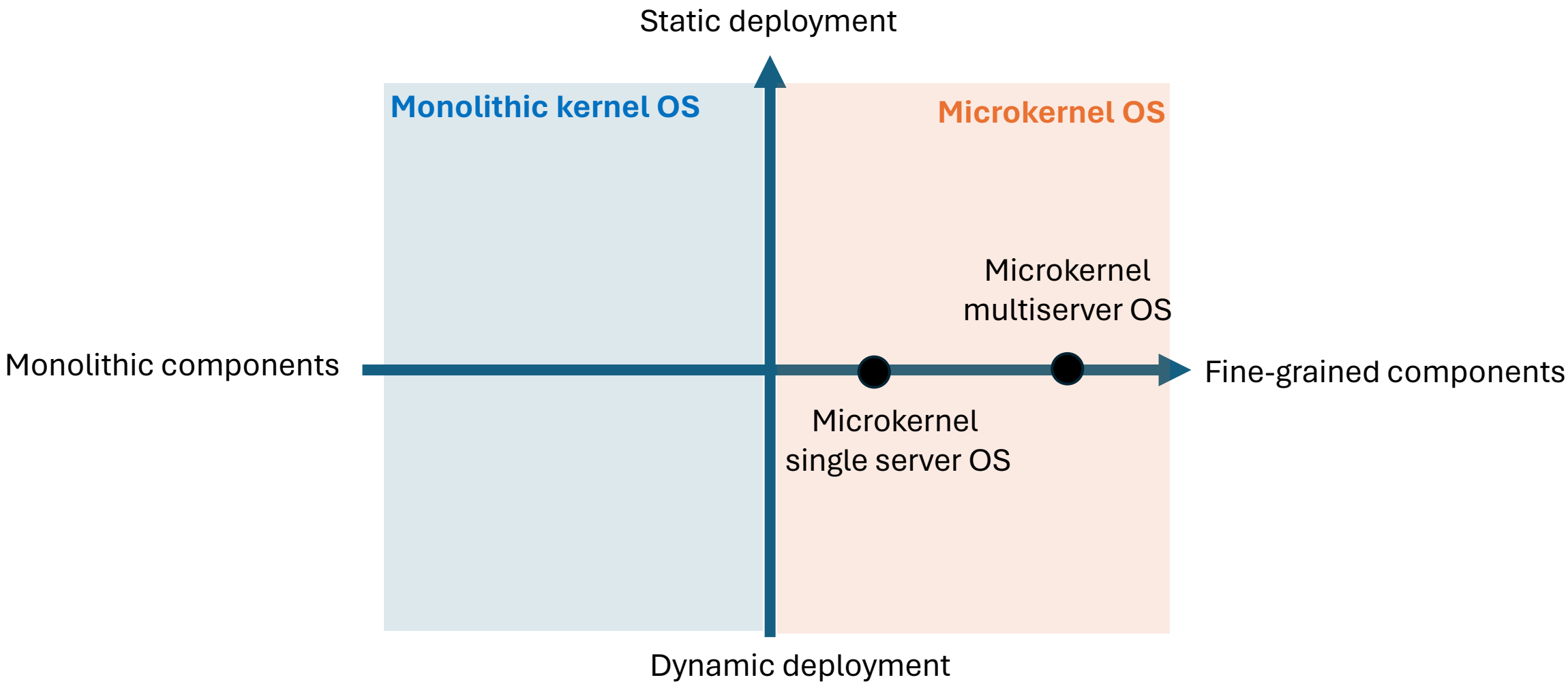


Source: https://www.baeldung.com

Monolithic Kernel vs. Microkernel

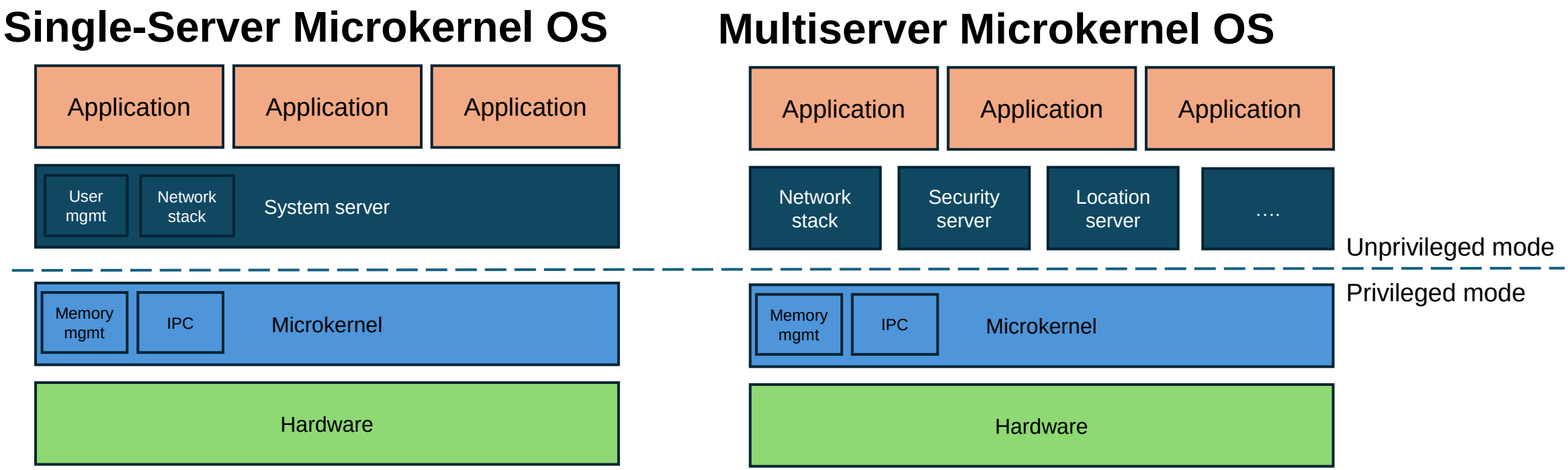
Monolithic kernel	Microkernel
Same address space	Separate address spaces
Configurability via compile-time options and parametrization	Configurability via different use (policy in user space)
Modularity via run-time dynamic linking	Modularity via extension in user space
Tight module coupling	Loose module coupling
OS is easier to implement	OS is more complex to implement
TCB is larger in size	TCB is smaller in size
If one component fails, the entire system crashes	If one component fails, it doesn’t affect the working of the microkernel

Microkernel OS Types



Source: Martin Děcký, *Microkernel-based and Capability-based Operating Systems*

Microkernel OS Types



Source: Martin Děcký, *Microkernel-based and Capability-based Operating Systems*

Security Aspects of Operating Systems

OS Security

= Ensuring: **C**onfidentiality, **I**ntegrity, **A**vailability **(CIA)**

= Aims to protect everything within the system

= Protects system resources including CPU, memory, disk, programs, and data

Importance

- Flaws lead to vulnerabilities in software
- Protecting sensitive data, ensuring integrity and user privacy
- Essential against cyber threats
- Lots of money has been lost

Who are the Attackers?

For example:

- Hackers **driven by the challenge**
- Insiders seeking **revenge** or gain **informal benefits**
- Criminals seeking **financial** gain
- Terrorist groups or nation states trying to **influence national policy**
- Agents seeking information for **economic, political purposes**

What are the Vulnerabilities?

Security vulnerabilities that affect the operating system:

- Automatically running active content
- Open ports
- Incorrect configuration
- Backdoor
- Unencrypted communication
- Limited resources
- Vulnerabilities in software

Security Goals

Authentication	Verifying the identity of users or systems
Authorization	Granting or denying access to resources
Data confidentiality	Ensuring that sensitive information is protected
Integrity	Ensuring the accuracy and reliability
Availability	Ensuring consistently accessibility

How can this be implemented?

How to ensure Operating System Security?

Built-in security

Additional security measures

Built-in Security

Hardware access control:

- Operating system regulates hardware access for processes
- Prevents one process from compromising another's security

Control of operating system services:

- Monitoring and control of services
- For example: file systems, memory management, and interprocess communication
- Control over system calls:
  - Processes access system services through system calls
  - OS monitors system calls, determining process authorization

Additional Security Measures

Further security improvement by:

- Configuring security settings
- Regular updates and patches
- Installing security software
- Security auditing and monitoring
- Supply chain management
- User training and awareness

Microkernel Architecture and Security

Motivation

“Operating-system structure has a strong effect on security. 96% of critical Linux exploits would not reach critical severity in a microkernel-based system, 57% would be reduced to low severity.”

“From the security point of view, the monolithic OS design is flawed.”

Source: https://trustworthy.systems

Security Aspects

- Only necessary permissions
- Secure inter-process communication
- Minimizes attack surface
- Reduce impact of security vulnerabilities

Additional Security Measures

- Only necessary permissions
- Secure inter-process communication
- Minimizes attack surface
- Reduce impact of security vulnerabilities
- Secure implementation
- Secure service design
- Security monitoring

seL4 Microkernel

Secure embedded L4:

- Provides security guarantees at OS and application levels
- Only the kernel operates in privileged mode
- Focus on formal verification

Basis:

- For various OS and runtime environments
- For example: Genode OS Framework

Source: http://www.microkernel.info/

Genode

- Tool kit for building operating systems
- Open-ended framework
- Microkernel architecture

Integration of seL4 in Genode:

- Genode provides a platform on which various microkernels can be run
  - Including seL4
- Using the security features and formal verification of seL4
- Retaining flexibility and modularity of Genode framework

Genode

Genode can be operated on various **microkernels**

For example:

- seL4 Microkernel
- NOVA Microhypervisor
- Muen Separation Kernel
- In-House Development

More Operating Systems

Escape

Fuchsia

M³

M³

MINIX 3

L4
Re

L4Re

Helen OS

Source: http://www.microkernel.info/

Dresden, January 16, 2024

“The operating system **L4Re** Secure Separation Kernel has been approved by the German Federal Office for Information Security (BSI) for the processing of classified information up to classification level German GEHEIM”

Source: https://www.kernkonzept.com

Security Focused Operating Systems

Secure OS’s

Two types of secure OS’s:

- Security-**focused** OS
  - Implements measures like sandboxing, compartmentalization, and cryptographic isolation
  - Examples: Qubes OS

- Security-**evaluated** OS
  - Certified by security-auditing organizations
  - Examples: SUSE Linux, Windows 10 Enterprise

Qubes OS

- Free and open-source operating system
- Based on Xen Hypervisor
- Uses virtual machines to run applications in separate environments
- Rely on the isolation for protection

- Designed with a **focus on security**:
  - Implements secure components called qubes
  - Efficient isolation of tasks and applications
  - Minimizing the impact of vulnerabilities

Qubes OS and Microkernel

- Qubes OS is not microkernel-based
- BUT...

QubesOS/qubes-issues

#3894 **Use verified L4 kernel instead of Xen**

24 comments

 **GWeck** opened on May 12, 2018

Source: https://github.com

Some CVEs

CVE-2015-4001

Problem:

- Security vulnerability in the OZWPAN driver
- Error: Integer signedness error → negative result from subtraction
- Threatened the security of Linux systems:
  - Denial of service
  - Execution of arbitrary code with kernel privileges

Mitigation by microkernel:

- Driver runs as a server at user level in a separate address space
- Isolation from the kernel prevents direct access to its memory

CVE-2014-9803

Problem:

- Security vulnerability on certain Nexus devices
- Error: Incorrect handling of execute-only pages
- Threatened the security of Linux systems:
  - Allowing an application to gain kernel privileges

Mitigation by microkernel + formal verification:

- This operation must occur in kernel mode → possible in microkernel
- Formal verification ensures the correctness of the microkernel's implementation → not possible in formally verified microkernel

CVE-2015-8961

Problem:

- Security vulnerability in the ext4_journal_stop function
- Error: Unauthorized access to a specific error field
- Threatened the security of Linux systems:
  - Full file system disclosure or a kernel crash
  - Posing significant risks to system integrity and data security

Partial mitigation by microkernel architecture:

- File system is implemented as a user-level server
  - No kernel crash, as the file system operates independently
  - Still allow to gain access to files, compromising data confidentiality

Summary

Summary

OS security crucial for OS and its applications

Microkernel architecture can boost security

Security-focused OS's demonstrate robust security through microkernel

Microkernel are not the key for general security

Sources

Sources

- Microkernel
  - https://learning.oreilly.com/library/view/software-architecture-patterns/9781098134280/ch04.html
  - https://learning.oreilly.com/library/view/operating-system-design/9781439881118/chapter-08.html
  - http://www.microkernel.info/
  - Martin Děcký, Microkernel-based and Capability-based Operating Systems

Sources

- OS & Security
  - https://www.techopedia.com/definition/24774/operating-system-security-os-security
  - https://pages.cs.wisc.edu/~remzi/OSTEP/security-intro.pdf
  - https://ics.uci.edu/~goodrich/teach/cs201P/notes/Ch03-OSSec.pdf
  - http://ndl.ethernet.edu.et/bitstream/123456789/87933/8/Chapter%20-%207.pdf
  - https://www.tutorialspoint.com/operating_system/pdf/os_security.pdf
  - https://www.researchgate.net/publication/372803341_Secure_Operating_System

Sources

- Microkernel & Security
  - https://trustworthy.systems/publications/full_text/Biggs_LH_18.pdf
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9653483
  - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9900222
  - https://www.researchgate.net/publication/241623590_Measures_to_improve_security_in_a_microkernel_operating_system
  - https://sel4.systems/
  - https://genode.org/
  - https://l4re.org/

Sources

- Security Focused Operating Systems
  - https://en.wikipedia.org/wiki/Security-focused_operating_system
  - https://www.stationx.net/secure-operating-systems/
  - https://www.qubes-os.org/

- CVE
  - https://blogs.blackberry.com/en/2020/09/study-confirms-that-microkernel-is-inherently-more-secure
  - https://microkerneldude.org/2018/08/23/microkernels-really-do-improve-security/
  - https://trustworthy.systems/publications/full_text/Biggs_LH_18.pdf