FCC compliance with open source:
Running OpenWrt in a VM on top of the L4Re microhypervisor

Michael Hohmuth

Kernkonzept

MICROKERNEL MADE IN GERMANY

FCC Wifi rule

2014: New FCC rule

Router manufacturers need to prevent Wifi misconfiguration

Prevent misuse of unlicensed / restricted frequency spectrum

Compatibility with open-source router OSes?

Ouch!

prpl Foundation's idea

2015: Virtualization is here!

Can we use it to isolate the Wifi driver from the open-source OS?

Let's do a proof of concept ...

A prpl cocktail: Ingredients

A core of MIPS

- MIPS P5600: Imagination Technologies

An extension of virtualization

- MIPS VZ: Imagination Technologies

An SoC of audacity

- Baikal T platform: Baikal Electronics

A hypervisor of open source

- L4Re microhypervisor: Kernkonzept

A router OS of choice

- OpenWrt

A bag of guts

- Sponsorship: prpl Foundation

A teaspoon of luck …

Stir. Serve hot.

About Kernkonzept

Develops and supports the open-source L4Re operating system

L4Re Microhypervisor / Microkernel

- Minimal secure real-time separation kernel

L4Re UVMM

- For hardware-assisted virtualization with minimal Trusted Computing Base (TCB)

L4Re Runtime Environment

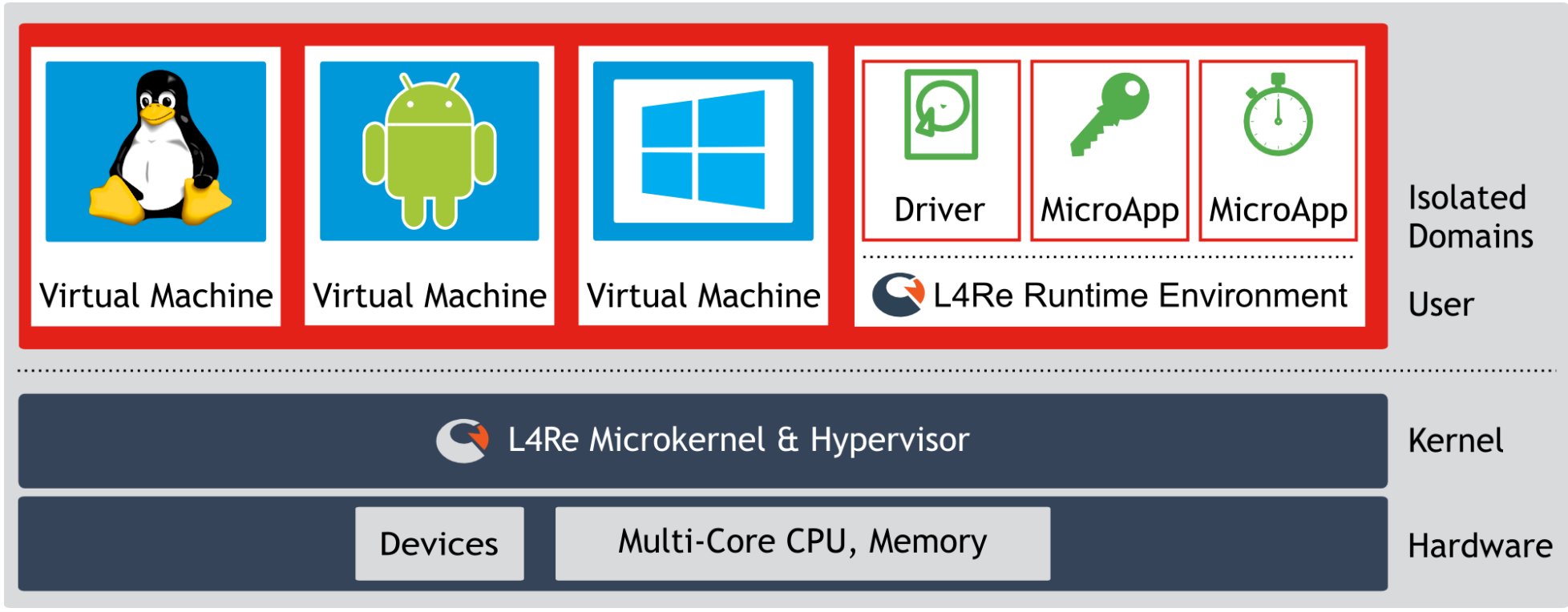
- For native trusted apps with minimal TCB

L4Linux, L4Android

- Paravirtualization solutions

Based in Dresden, Germany

L4Re operating system overview



Why virtualization on the router?

Integration of untrusted third-party components

Home automation, home security, media streaming

Separate development / update cycles integrated components

DECT / LTE / SNMP

Smaller attack surface for secrets kept on the router

VPN keys, admin passwords

Isolating critical gateway / router part from other components to reduce attack surface

Wifi AP, telephony, printer, family settings, local storage, private cloud

Isolate proprietary / dusty deck components

For licensing reasons, or to limit attack surface

FCC Wifi rule …

Virtualization vs Linux container solutions

Smaller trusted computing base (TCB)

Small = good

- Studies: 20-50 bugs per 1000 lines of code

Several orders of magnitude smaller

- Much lower probability of 0day events

Native trusted microapps

Real time and security

Linux is off the trusted path

Larger footprint

RAM: ~ 5 MB for hypervisor / VMM
~ 5 MB for each additional Linux

Harder to set up and manage

Dynamic / automatic deployment is a WIP

A prpl cocktail: Ingredients

A core of MIPS

- MIPS P5600: Imagination Technologies

An extension of virtualization

- MIPS VZ: Imagination Technologies

An SoC of audacity

- Baikal T platform: Baikal Electronics

A hypervisor of open source

- L4Re microhypervisor: Kernkonzept

A router OS of choice

- OpenWrt

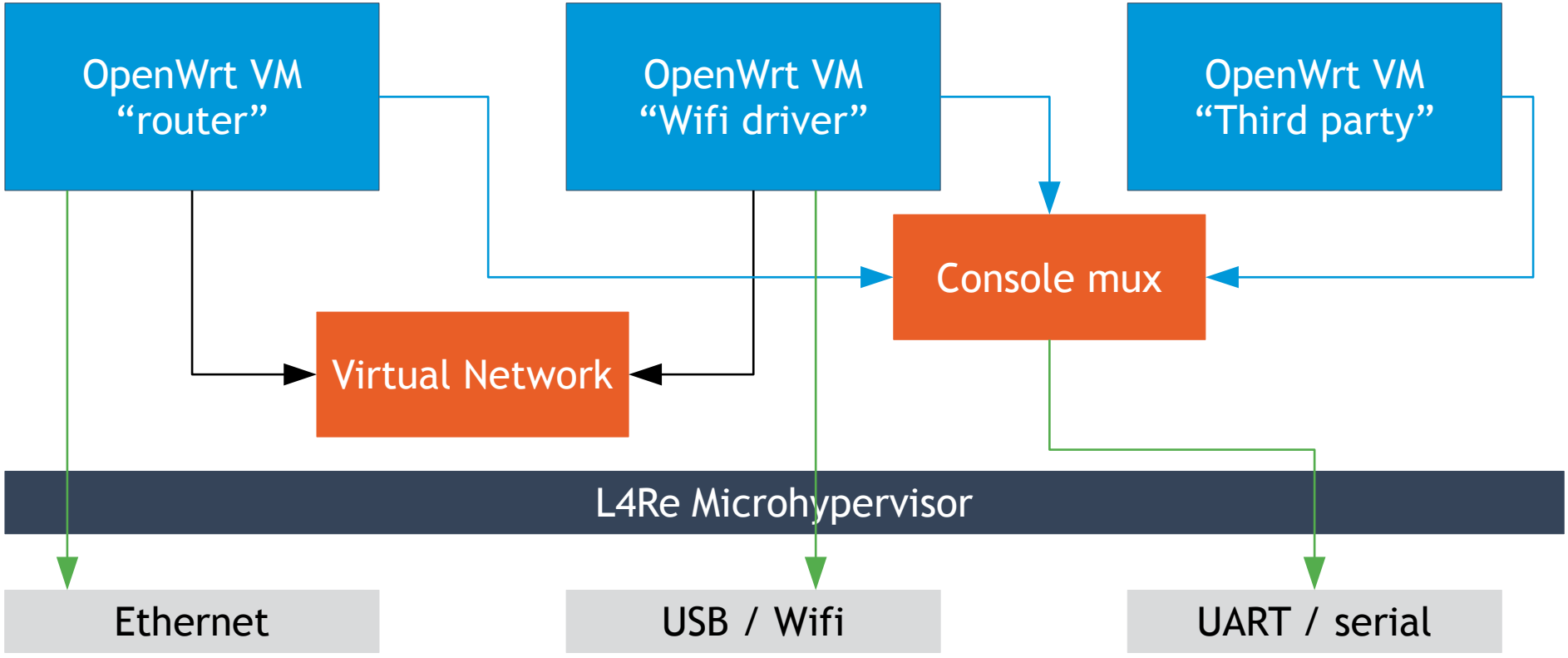
A bag of guts

- Sponsorship: prpl Foundation

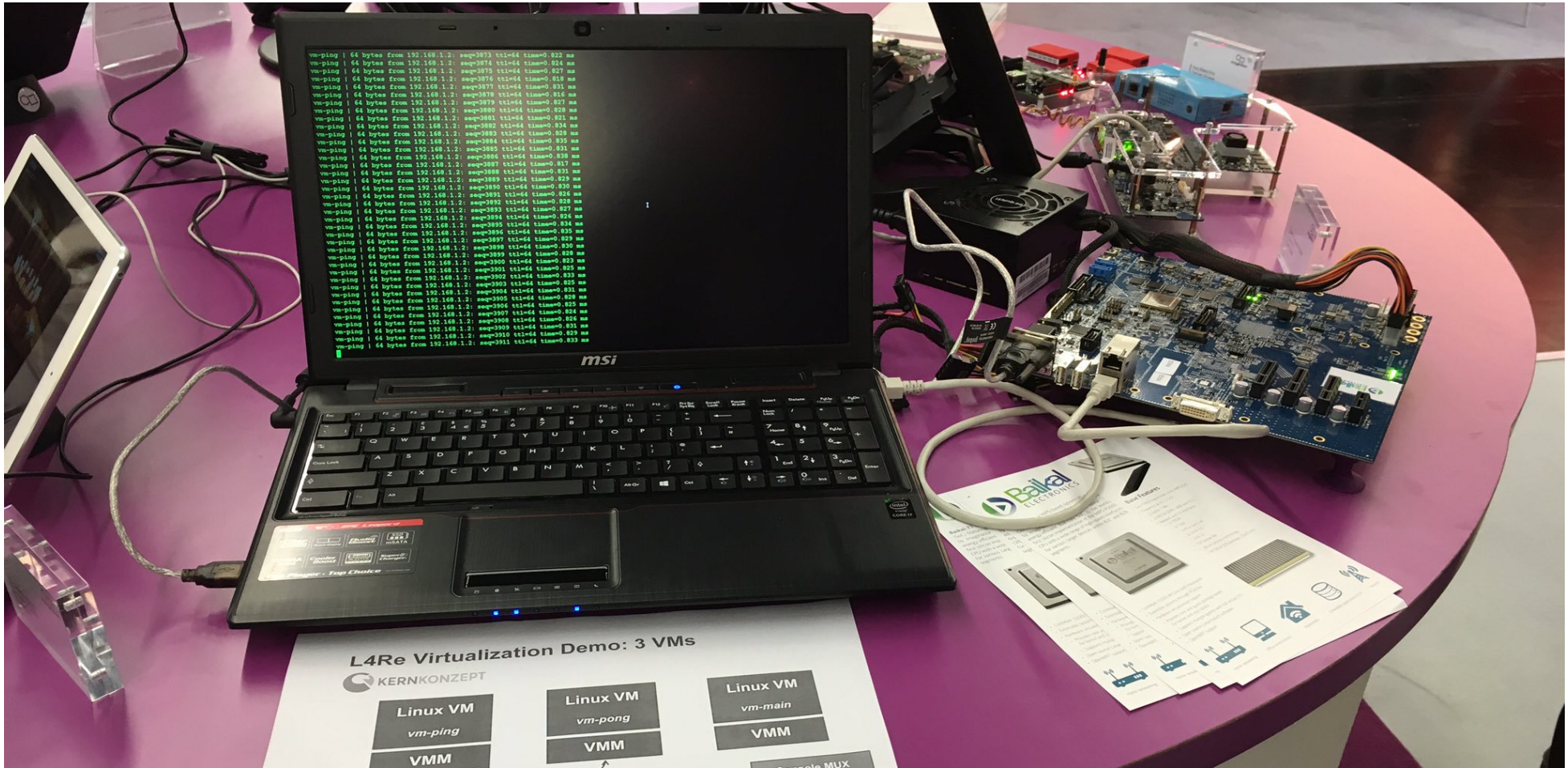
A teaspoon of luck …

Stir. Serve hot.

prpl Wifi router demo



It works


msi
L4Re Virtualization Demo: 3 VMs
KERNKONZEPT
Linux VM
vm-ping
VMM
Linux VM
vm-pong
VMM
Linux VM
vm-main
VMM
Baikal
ELECTRONICS

War stories

We have virtualization? Oh yeah, right …

Accidentally, it appears

The joys of evaluation hardware

Flaky power supply, flaky network boot, errata, frequent firmware updates

Version / life cycle issues

L4Re UVMM, Baikal platform, and OpenWrt all have different Linux kernel version requirements

A bunch of Wifi dongles

Find a Wifi dongle that's supported by the selected Linux kernel *and* that's still on the market

Ironing out the bugs

In other people's software (mostly ;-)

Evaluation – FCC use case

What's there

CPU / MMU virtualization – MIPS VZ

Open source L4Re Microhypervisor

Virtual MIPS platform for Linux

Device pass-through into VMs

OpenWrt virtualization

Virtual networking among VMs

Untrusted third-party VMs

What's missing

IOMMU (SMMU) support – missing on the Baikal platform

Secure boot (vs open source …)

VM management

Virtual platform standard for MIPS / x86

Summary

Virtualization is coming your way

Telcos / service providers want it

Use cases

Third-party software, security, life-cycle management

Don't get worked up about the FCC rule …

Next steps

Integration of container technology and (real) virtualization

SoC vendor support for hypervisors

KERNKONZEPT

Thank you!

www.kernkonzept.com

MICROKERNEL MADE IN GERMANY

KERNKONZEPT

Backup

www.kernkonzept.com

MICROKERNEL MADE IN GERMANY

L4Re core features

x86, ARM, MIPS; 32- or 64-bit systems

Native apps with minimal TCB

Strong temporal and spatial isolation: real-time & secure

Dynamic or static setups

Supports hardware-assisted and para-virtualization

Run VMM as untrusted user-mode applications

Open source

Mature OS (developed since 1997)

L4Re applications

High-assurance security

Dual-use laptops, VPN gateways, secure exchange gateways, data diodes

Open and secure mobile systems

Smart phones, tablet devices: Open systems with strong security requirements

Industrial monitoring and control

Virtualization of legacy components for consolidation

Car infotainment

Consolidation of trusted and untrusted components

Open software stack (“apps”)

Cloud security

Trusted virtualization solutions

Kernkonzept services

Consulting

Helping customers to use the L4Re system in their own products and solutions

Contracting / maintenance

Develop and maintain L4Re-based software

Licensing

Open-source or commercial L4Re licenses available