



\Orchestrating a brighter world

NEC

Severely Debloating Cloud Images with Unikraft

Sharan Santhanam <sharan.santhanam@neclab.eu>

Felipe Huici <felipe.huici@neclab.eu>

Alex Jung <a.jung@lancs.ac.uk>

Simon Kuenzer <simon.kuenzer@neclab.eu>

FOSDEM 2021

This work has received funding from the European Union's Horizon 2020 research and innovation program under grant agreements no. 871793 ("ACCORDION") and 825377 ("UNICORE"). This work reflects only the author's views and the European Commission is not responsible for any use that may be made of the information it contains.



Specialization = High Performance

■ Networking

- ℓ Sandstorm
- ℓ Minicache
- ℓ ClickOS

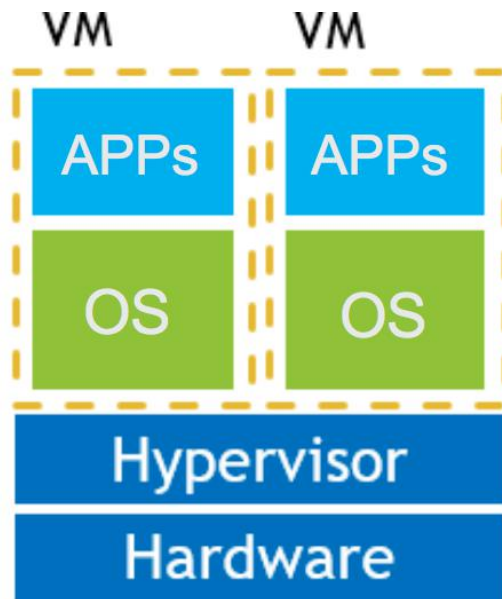
■ Efficient run-time environments

- ℓ MirageOS
- ℓ Ling
- ℓ runtime.js

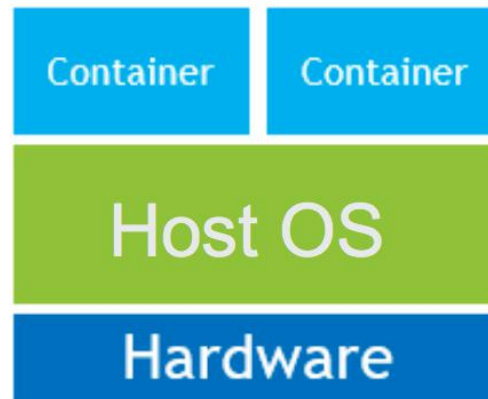
■ Hardware

- ℓ TPUs
- ℓ Movidius
- ℓ FPGAs

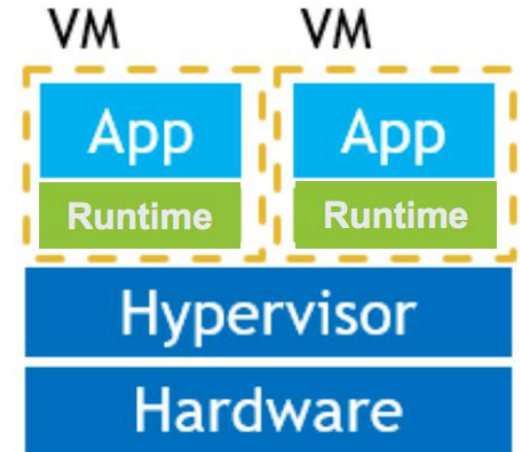
Background: Unikernels



Virtual Machines



Linux Containers



Unikernels

The Potential of Unikernels



■ Fast instantiation, destruction and migration time

- ℓ 10s of milliseconds or less (and as little as 2.3ms)
(*LigthVM [Manco SOSP 2017]*, *Jitsu [Madhvapeddy, NSDI 2015]*)



■ Low memory footprint

- ℓ Few MBs of RAM or less (*ClickOS [Martins NSDI 2014]*)



■ High density

- ℓ 8k guests on a single x86 server (*LigthVM [Manco SOSP 2017]*)



■ High Performance

- ℓ 10-40Gbit/s throughput with a single guest CPU
(*ClickOS [Martins NSDI 2014]*, *Elastic CDNs [Kuenzer VEE 2017]*)



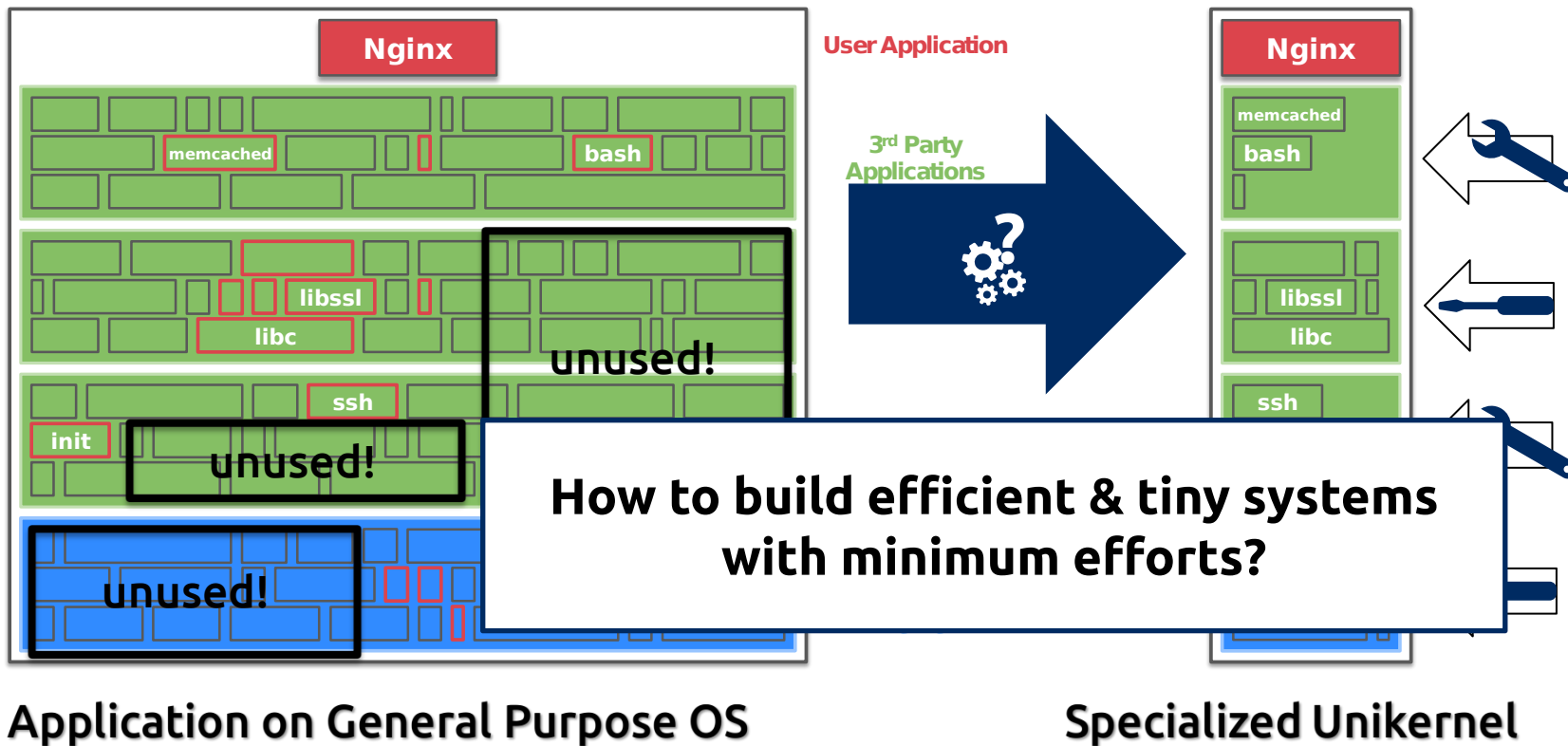
■ Reduced attack surface

- ℓ Small trusted compute base
- ℓ Strong isolation by hypervisor

Unikernels in Action

- Today OS/VM/container:
lots of unnecessary code
= *lots* of overhead,
big attack vector

- Specialized System: only what's needed
is there *but lots* of development time!
(has to be done manually,
may require changing code)

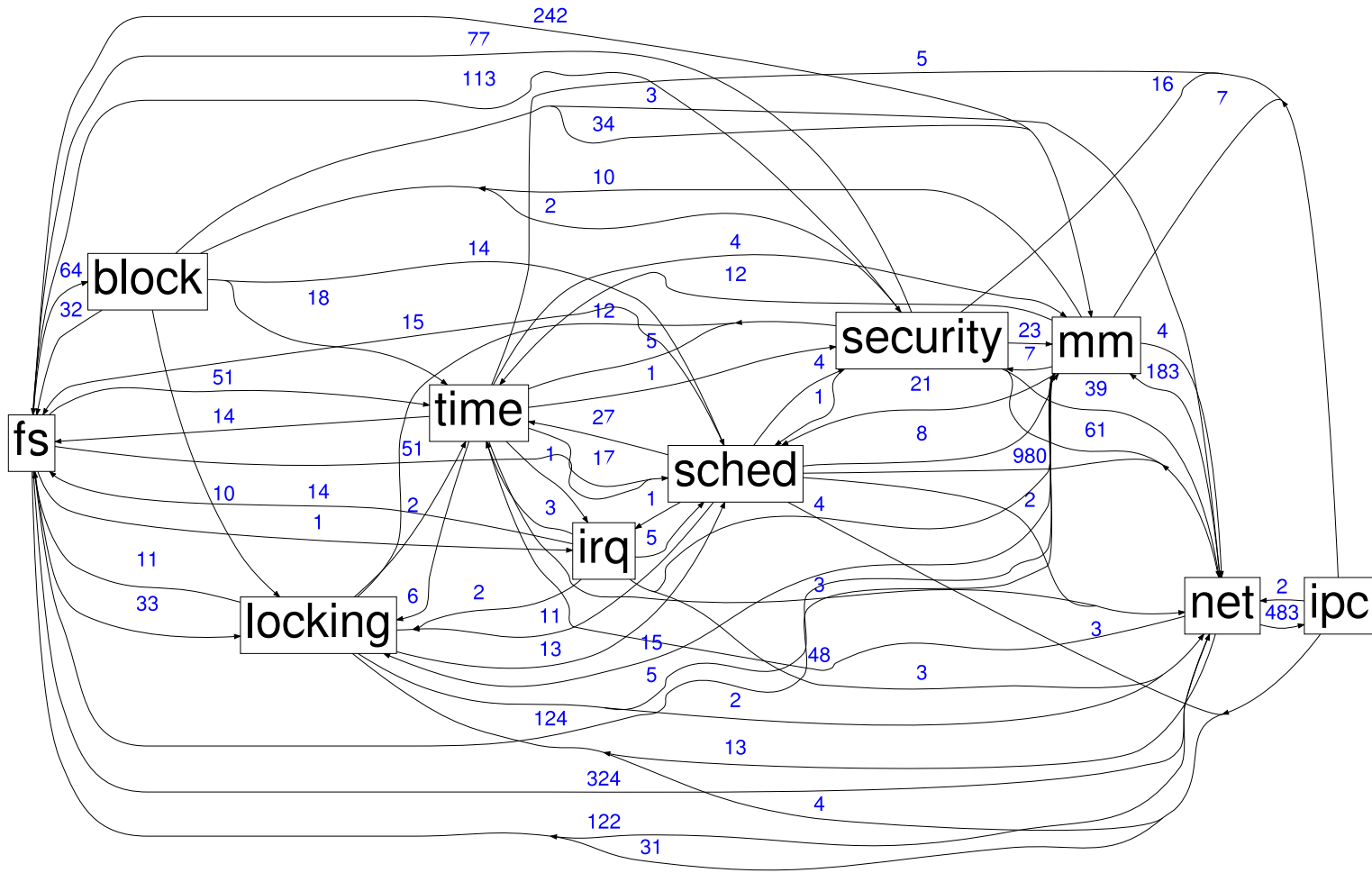


Unikernel: Dichotomy of Performance and Portability

(1) Transparently: *applications are ported and automatically benefit from lower boot times, less memory consumption, etc.*

(2) Modified: *applications are hooked into high performance APIs at the right level in the software stack*

Ofcourse, let me use Linux?



Then, maybe existing unikernels?

(1) They require significant expert work to build and to extract high performance; such work has to for the most part be redone for each target application.

(2) They are often non-POSIX compliant, requiring porting of applications and language environments.

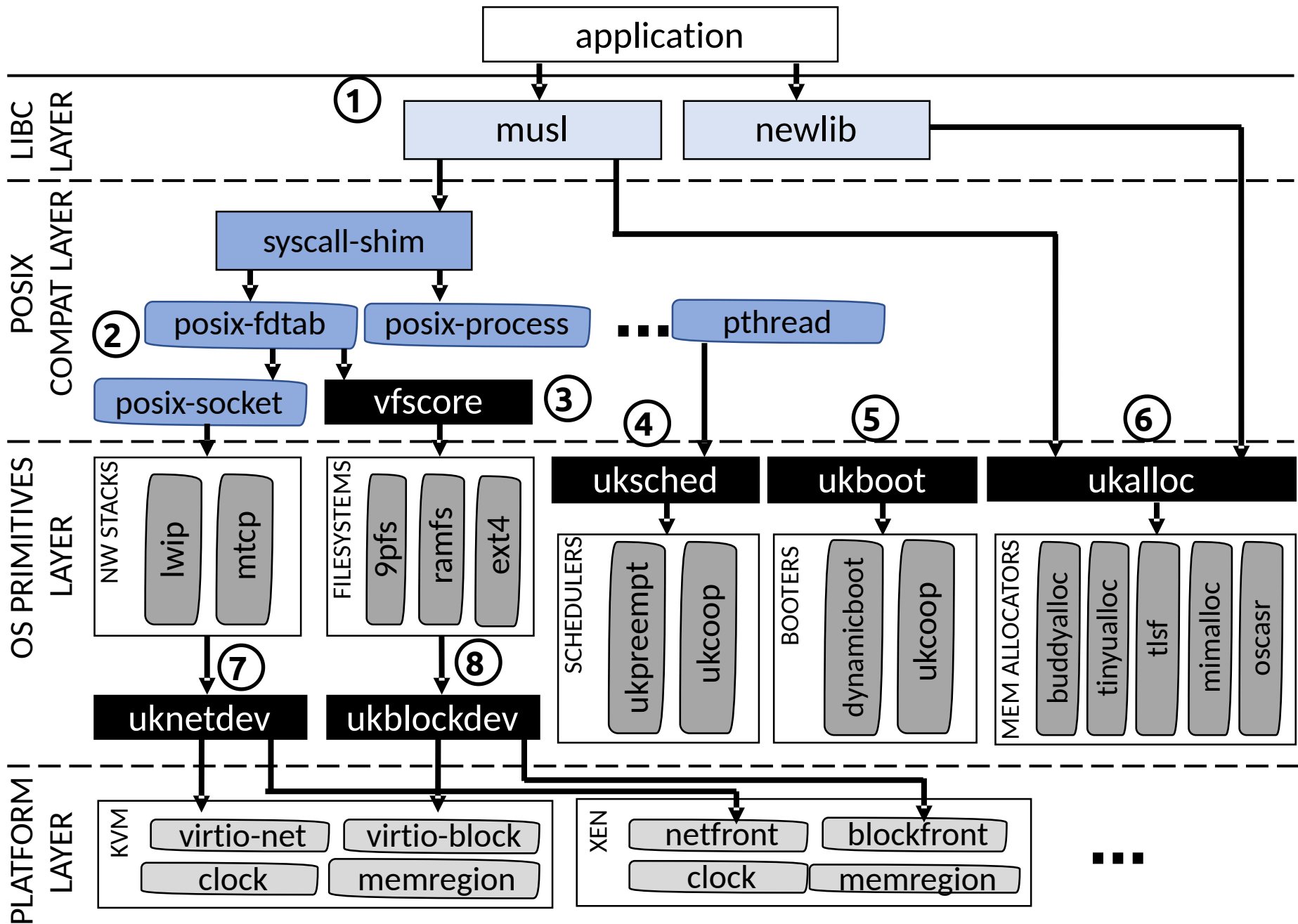
(3) The (uni)kernels themselves, while smaller, are *still* monolithic and hard to customize

Motivation

- Support wide range of use cases
- Simplify building and optimizing
- Simplify porting of existing applications
- Common and shared code base for Unikernel projects: “win-win”
- Support for many hypervisors, bare-metal nodes, and CPU architectures



- Concept: “Everything is a library”
 - ℓ Decomposed OS functionality
- Two components:
 1. Library Pool
 2. Build Tool



Transparently: *applications are ported and automatically benefit from lower boot times, less memory consumption, etc.*

Unikraft: Run a Binary Compatible App

Platform	Routine call	#Cycles	nsecs
<i>Linux/KVM</i>	System call	604.62	232.55
	System call (no mitigations)	142.31	54.74
<i>Unikraft/KVM</i>	System call	85.0	32.69
<i>Both</i>	Function call	6.0	2.31

Table 1. Cost of binary compatibility/syscalls with and without security mitigations.

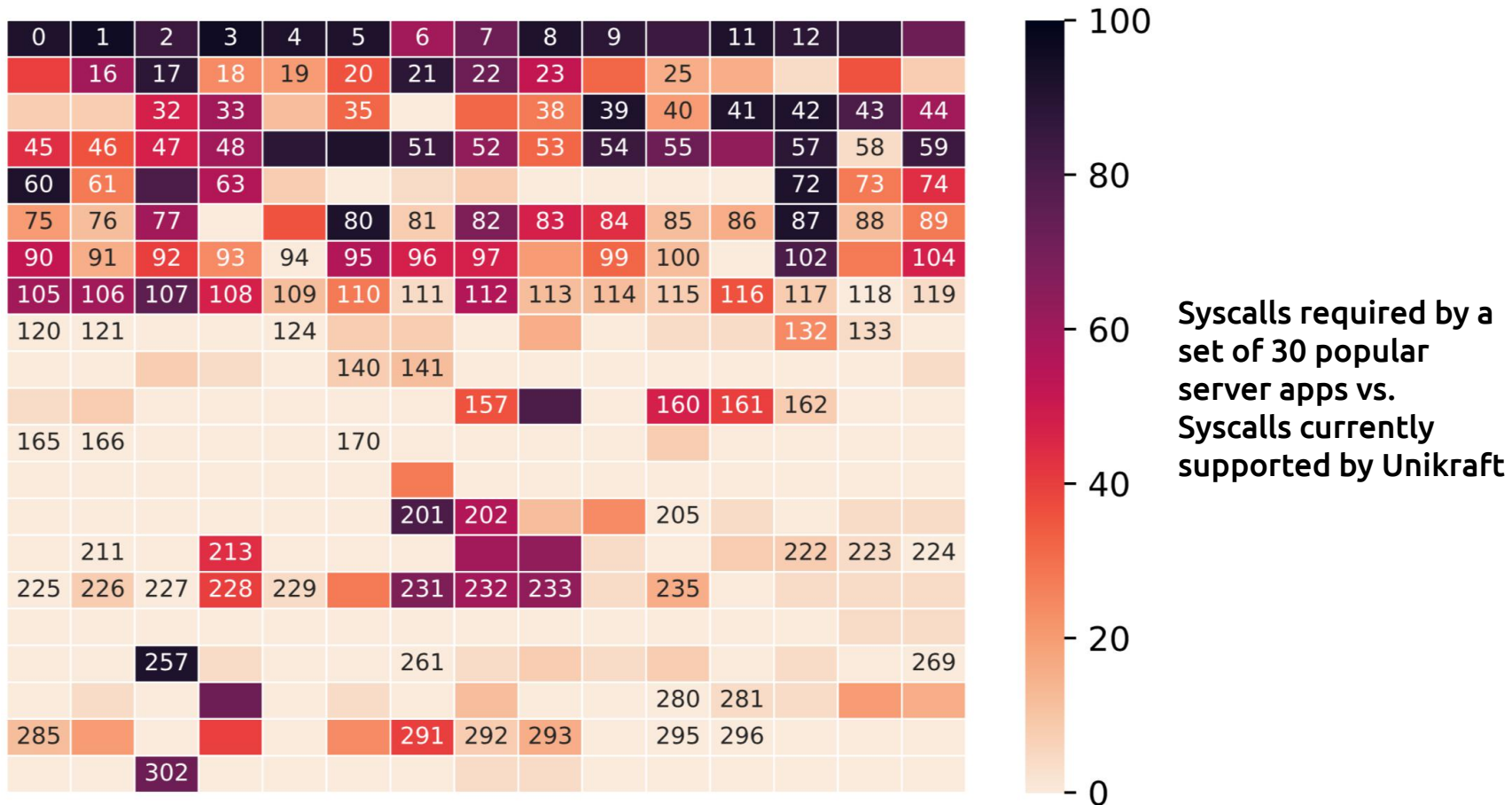
Unikraft: Compile an App Transparently



Compile Time

	musl			newlib		
	Size (MB)	std	compat. layer	Size (MB)	std	compat layer
lib-axtls	0.336	✗	✓	0.432	✗	✓
lib-bzip2	0.296	✓	✓	0.364	✗	✓
lib-c-ares	0.304	✓	✓	0.432	✗	✓
lib-ducktape	0.700	✓	✓	0.772	✗	✓
lib-farmhash	0.232	✓	✓	0.276	✓	✓
lib-fft2d	0.356	✓	✓	0.396	✗	✓
lib-helloworld	0.232	✓	✓	0.256	✓	✓
lib-libucontext	0.232	✓	✓	0.276	✓	✓
lib-libunwind	0.232	✓	✓	0.276	✗	✓
lib-lighttpd	0.796	✗	✓	0.916	✗	✓
lib-lighttpreply	0.256	✓	✓	0.296	✓	✓
lib-memcached	0.524	✓	✓	0.672	✗	✓
lib-micropython	0.527	✓	✓	0.628	✗	✓
lib-nginx	1.13	✗	✓	1.20	✗	✓
lib-open62541	0.248	✗	✓	0.804	✗	✓
lib-openssl	2.98	✗	✓	3.01	✗	✓
lib-pcre	0.344	✓	✓	0.380	✗	✓
lib-python	4.75	✗	✓	4.81	✗	✓
lib-redis-client	0.640	✗	✓	0.801	✗	✓
lib-redis-server	1.26	✗	✓	1.42	✗	✓
lib-ruby	6.84	✗	✓	6.93	✗	✓
lib-sqlite	1.22	✓	✓	1.31	✗	✓
lib-zlib	0.348	✓	✓	0.404	✗	✓
lib-zydis	0.276	✓	✓	0.328	✗	✓

What Unikraft *Could* Transparently Support

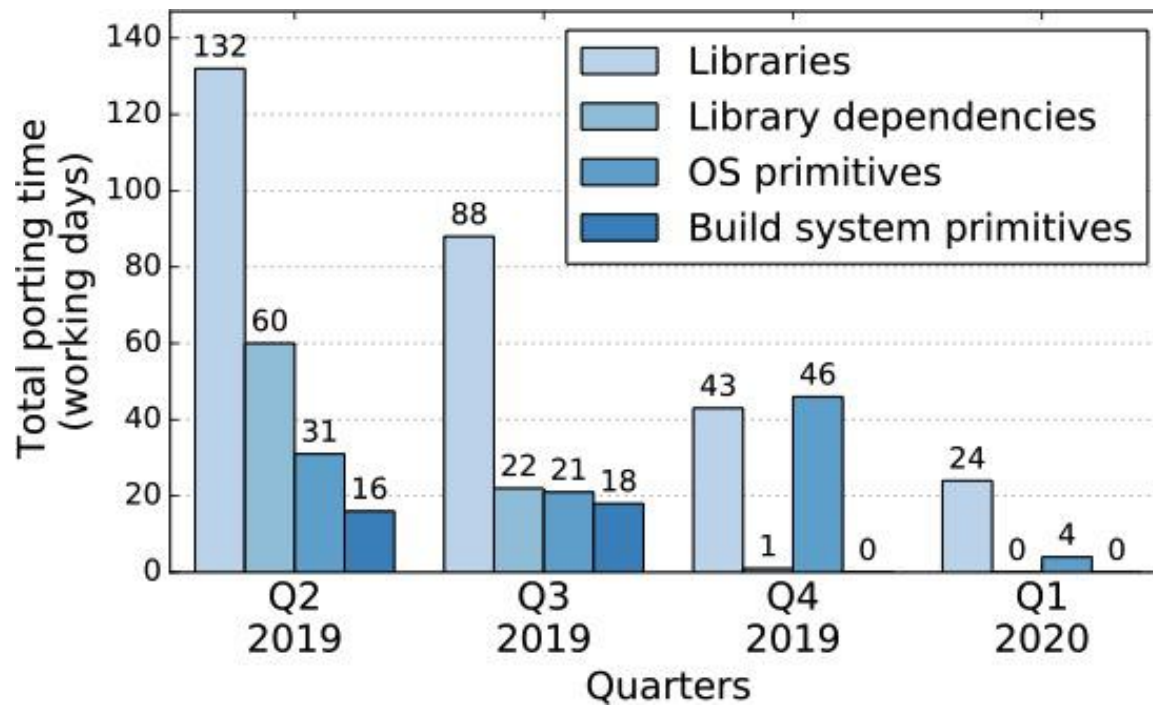


Modified: *applications are hooked into high performance APIs at the right level in the software stack*

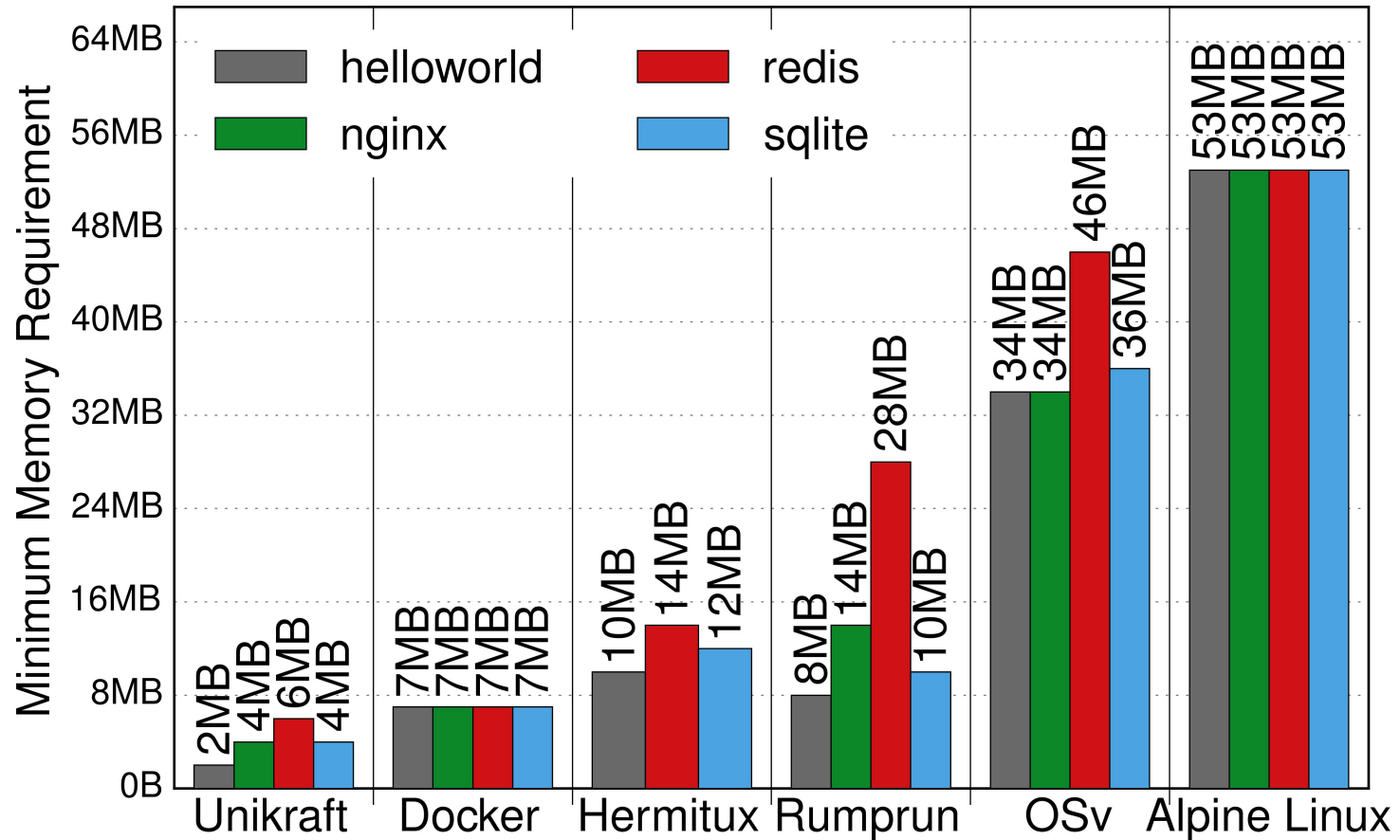
Unikraft: Native Support of Applications

Applications	NGINX, SQLite, Redis, memcached, Click modular router, lighttpd (ongoing).
Frameworks	Intel DPDK, TensorFlow Lite, PyTorch.
Compiled Languages	C/C++, Go, Web Assembly (WAMR), Lua, Java/OpenJDK (ongoing), Rust (ongoing)
Interpreted Languages	Python, Micropython, Ruby, JavaScript/v8 (ongoing).

Unikraft: Support yet another App



Unikraft: Memory Efficiency



Unikraft: Ease of Use

Unikraft is even easier to use!

kraft: a new companion tool!

- ℓ Improves user & developer experience
- ℓ Lists and clones available Unikraft libraries from GitHub organization
- ℓ Building and initial configuration
- ℓ Testing und Benchmarking
- ℓ Get <https://github.com/unikraft/kraft/>
- ℓ ..and start building your Unikernel:

```
> kraft update  
  
> kraft list  
  
> kraft init -a APPNAME  
> kraft build  
  
> kraft run -p kvm
```

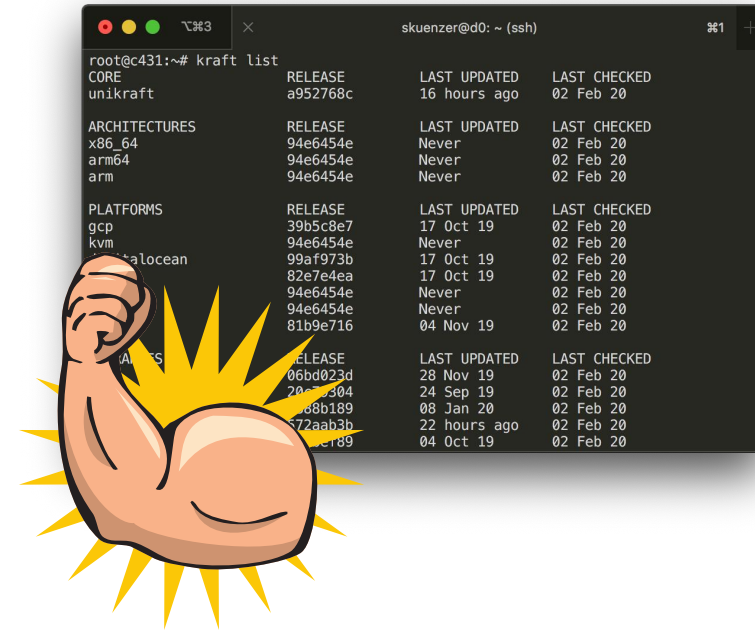
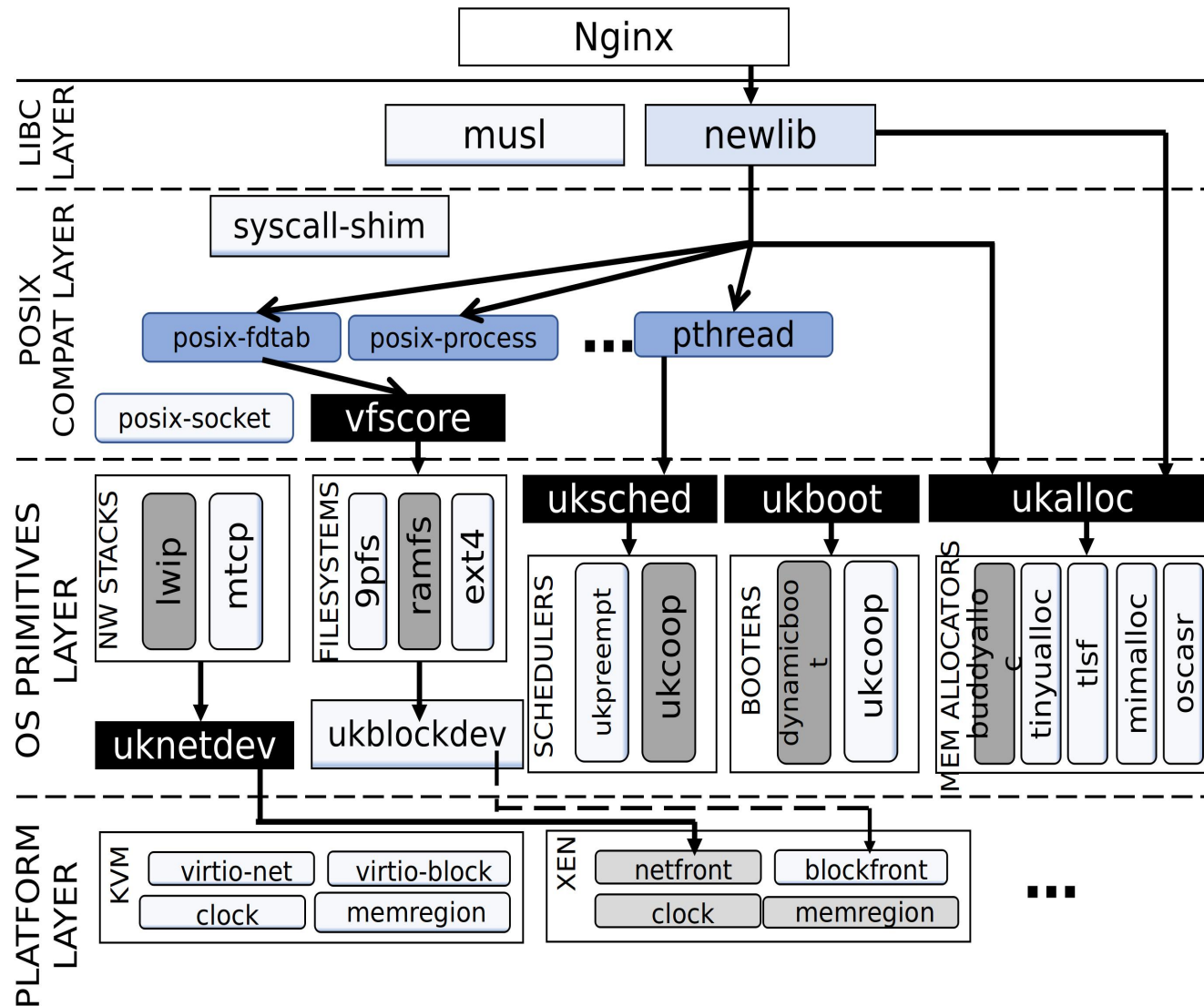


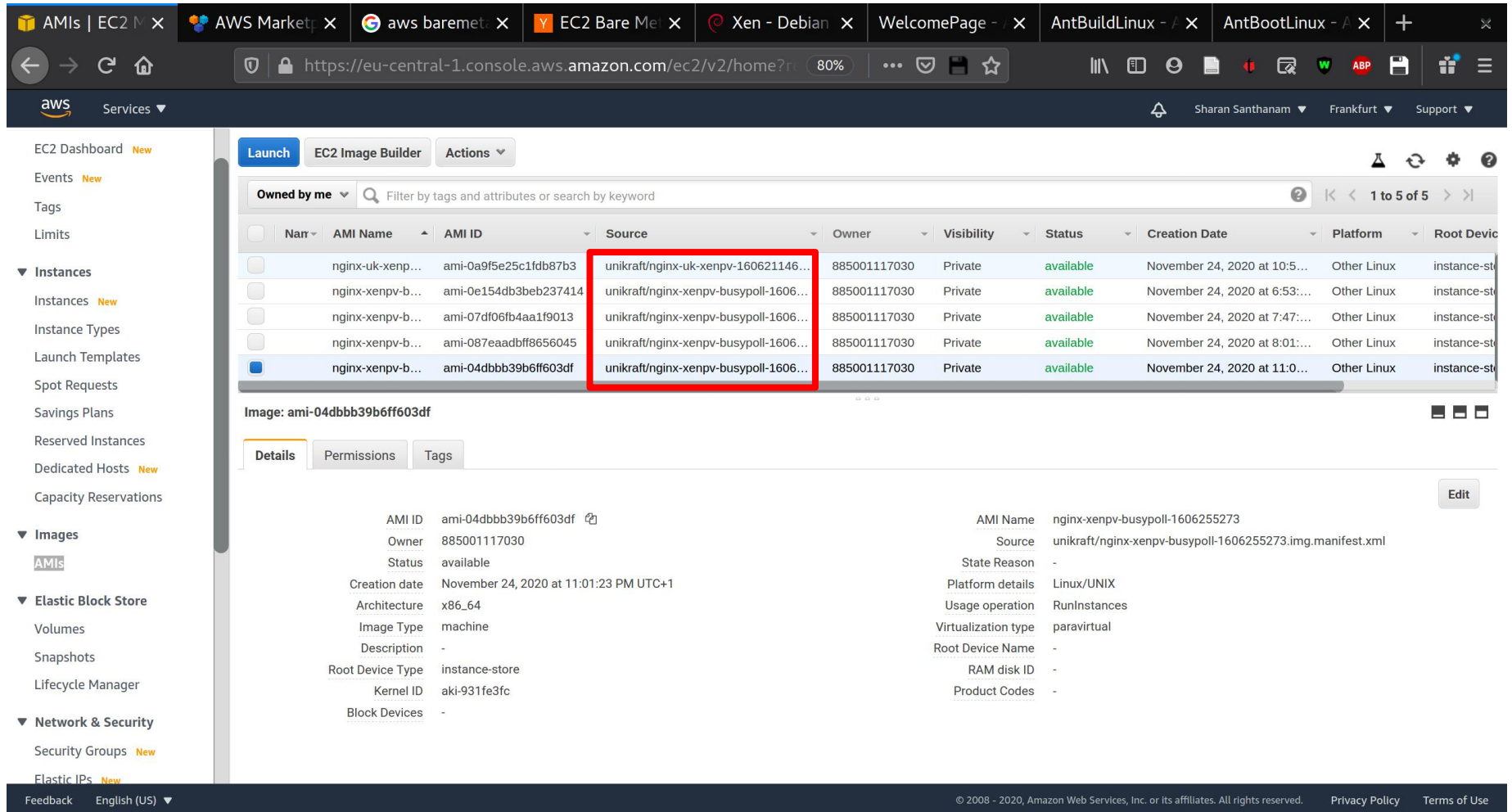
Image: <https://openclipart.org/detail/284486/strong-arm>

AWS Deployment

Unikraft: Nginx Port



Unikraft on AWS



The screenshot shows the AWS Management Console interface for the EC2 Image Builder service. The top navigation bar includes tabs for AMIs, EC2, AWS Marketplace, AWS Bare Metal, EC2 Bare Metal, Xen - Debian, WelcomePage, AntBuildLinux, and AntBootLinux. The left sidebar contains navigation links for EC2 Dashboard, Events, Tags, Limits, Instances, Images, Elastic Block Store, and Network & Security. The main content area displays the 'Owned by me' tab for the EC2 Image Builder console. A table lists the AMIs, with the AMI 'nginx-xenpv-busypoll-1606255273' highlighted. Below the table, the details for the selected AMI are shown, including its name, source, and various attributes.

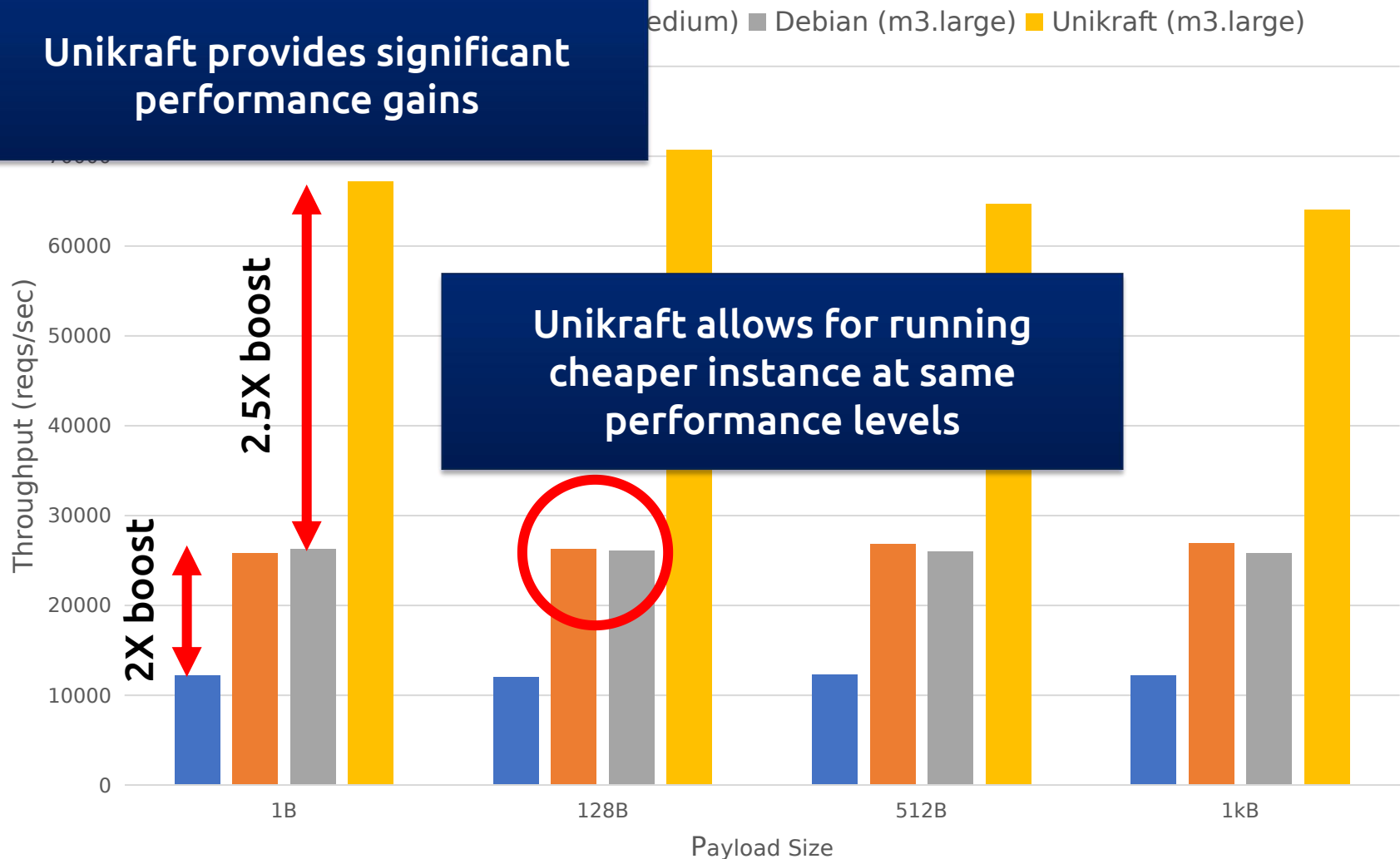
AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date	Platform	Root Device
nginx-uk-xenpv...	ami-0a9f5e25c1fdb87b3	unikraft/nginx-uk-xenpv-160621146...	885001117030	Private	available	November 24, 2020 at 10:53:...	Other Linux	instance-st...
nginx-xenpv-b...	ami-0e154db3beb237414	unikraft/nginx-xenpv-busypoll-1606...	885001117030	Private	available	November 24, 2020 at 6:53:...	Other Linux	instance-st...
nginx-xenpv-b...	ami-07df06fb4aa1f9013	unikraft/nginx-xenpv-busypoll-1606...	885001117030	Private	available	November 24, 2020 at 7:47:...	Other Linux	instance-st...
nginx-xenpv-b...	ami-087eaadbff8656045	unikraft/nginx-xenpv-busypoll-1606...	885001117030	Private	available	November 24, 2020 at 8:01:...	Other Linux	instance-st...
nginx-xenpv-b...	ami-04dbbb39b6ff603df	unikraft/nginx-xenpv-busypoll-1606...	885001117030	Private	available	November 24, 2020 at 11:01:...	Other Linux	instance-st...

Image: ami-04dbbb39b6ff603df

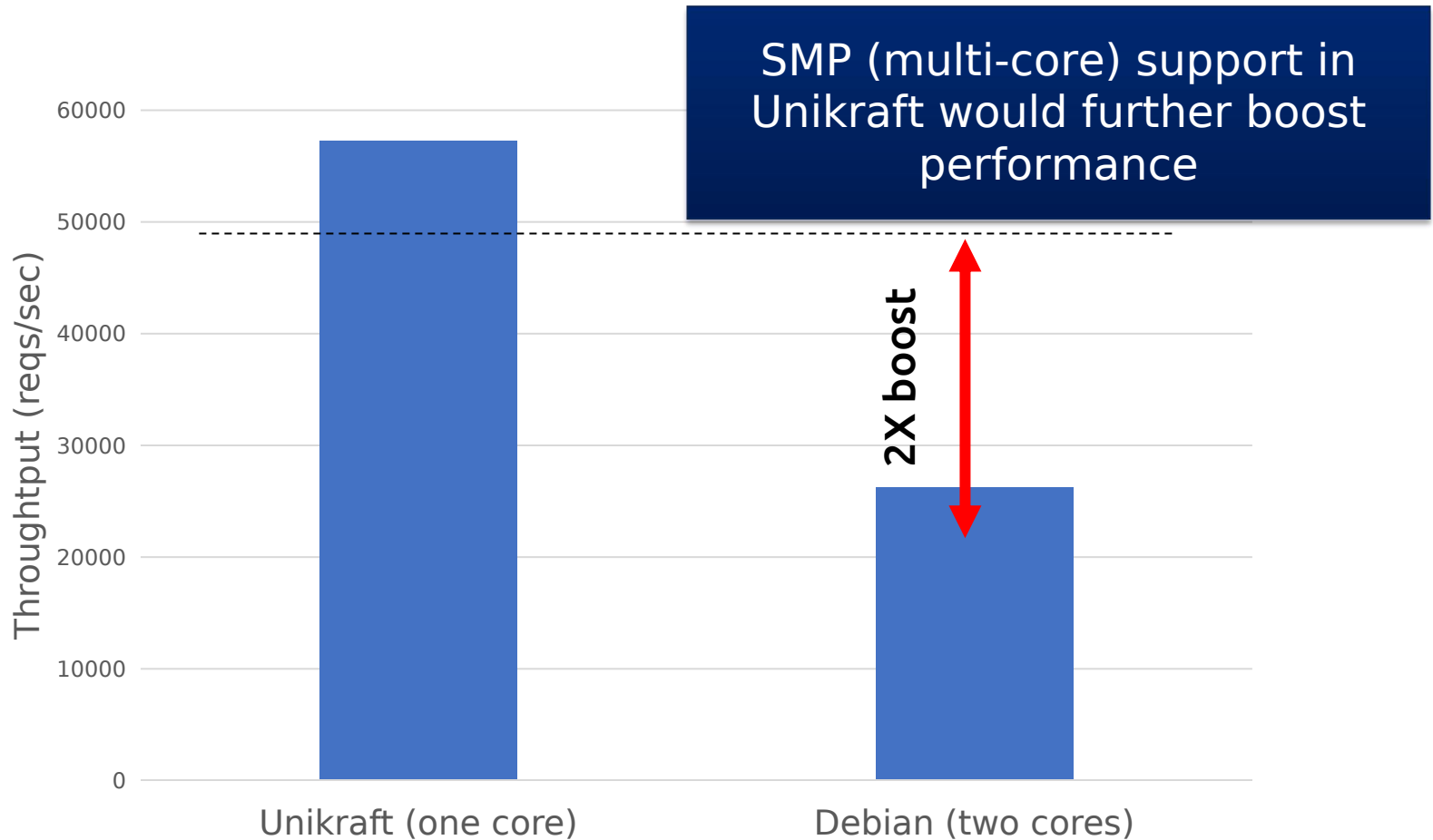
Details Permissions Tags

Property	Value
AMI ID	ami-04dbbb39b6ff603df
Owner	885001117030
Status	available
Creation date	November 24, 2020 at 11:01:23 PM UTC+1
Architecture	x86_64
Image Type	machine
Description	-
Root Device Type	instance-store
Kernel ID	aki-931fe3fc
Block Devices	-
AMI Name	nginx-xenpv-busypoll-1606255273
Source	unikraft/nginx-xenpv-busypoll-1606255273.img.manifest.xml
State Reason	-
Platform details	Linux/UNIX
Usage operation	RunInstances
Virtualization type	paravirtual
Root Device Name	-
RAM disk ID	-
Product Codes	-

Unikraft NGINX Throughput vs. Linux on AWS

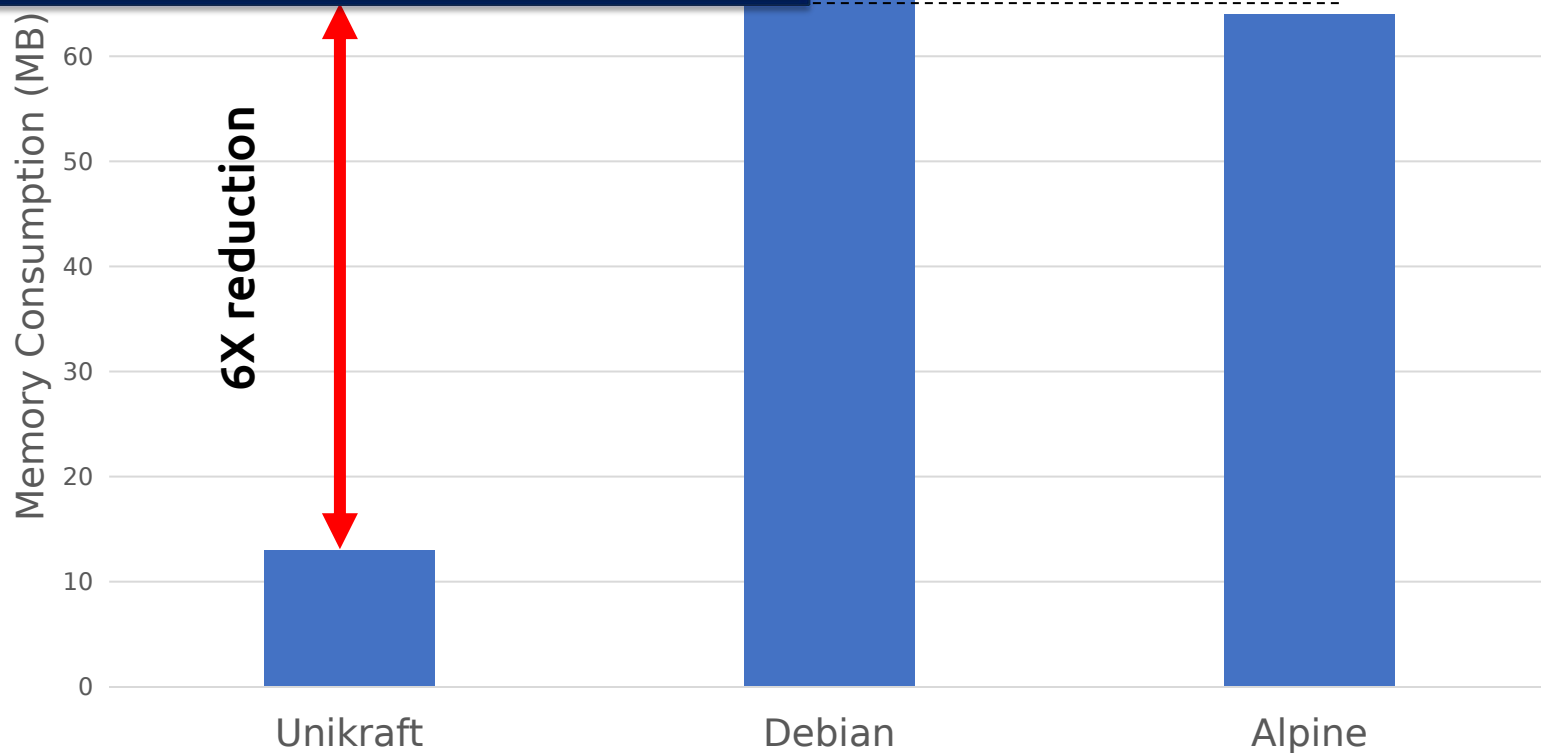


Unikraft Throughput vs. Linux: CPU Cores



Unikraft NGINX Memory Use vs. Linux on AWS

Could be leveraged to build our own hyper efficient Lambda services on AWS bare metal infrastructure





WordPress with NGINX and SSL Certified by Bitnami and Automattic

Version 5.5.3-1 on Debian 10 | Sold by [Bitnami](#)

★★★★☆ 11 AWS reviews

Bitnami, the leaders in application packaging, and Automattic, the experts behind WordPress, have teamed up to offer this official WordPress image on AWS Marketplace. WordPress with NGINX and SSL combines the world's most popular content management platform with the high performance and...

Linux/Unix, Debian 10 - 64-bit Amazon Machine Image (AMI)



NGINX Open Source Certified by Bitnami

Version 1.18.0-13-r07 on Debian 10 | Sold by [Bitnami](#)

81 external reviews ⓘ

NGINX Open Source is a lightweight and high-performance server capable of serving content to a high volume of connections. It is primarily adopted for its reliability, security, stability, and low resource consumption. It is used by high-demanding websites due to its asynchronous architecture and...

Linux/Unix, Debian 10 - 64-bit Amazon Machine Image (AMI)



NGINX Plus Basic - Amazon Linux AMI

Version 1.4 | Sold by [NGINX](#)

★★★★☆ 10 AWS reviews

Starting from \$0.34/hr or from \$2,500.00/yr (16% savings) for software + AWS usage fees

Deliver applications with performance, reliability, security, and scale with NGINX Plus on AWS. Deploy quickly and cost-effectively, and benefit from speeds <30ms. NGINX plus is the all in one (yet surprisingly lightweight) load balancer, reverse proxy, API gateway and content cache. Try it for...

Find us online



<https://github.com/unikraft>



<http://unikraft.org>



[<minios-devel@lists.xenproject.org>](mailto:minios-devel@lists.xenproject.org)

[<unikraft@listserv.neclab.eu>](mailto:unikraft@listserv.neclab.eu)



[@UnikraftSDK](https://twitter.com/UnikraftSDK)



Unikraft is a highly modular library pool and build system allowing users to seamlessly build extremely specialized and efficient images (VMs, containers, bare metal) targeting particular applications.



Orchestrating a brighter world

NEC brings together and integrates technology and expertise to create the ICT-enabled society of tomorrow.

We collaborate closely with partners and customers around the world, orchestrating each project to ensure all its parts are fine-tuned to local needs.

Every day, our innovative solutions for society contribute to greater safety, security, efficiency and equality, and enable people to live brighter lives.