Morello Linux

Technical Update

Vincenzo Frascino
Morello Software Architect@ARM
19/04/2024

Morello Linux Agenda

- “Our Motto”
- Status of Morello Linux
- Integration Drop 1.8 – April 2024
- What’s next? Future opportunities for the Ecosystem Research
- Our Community

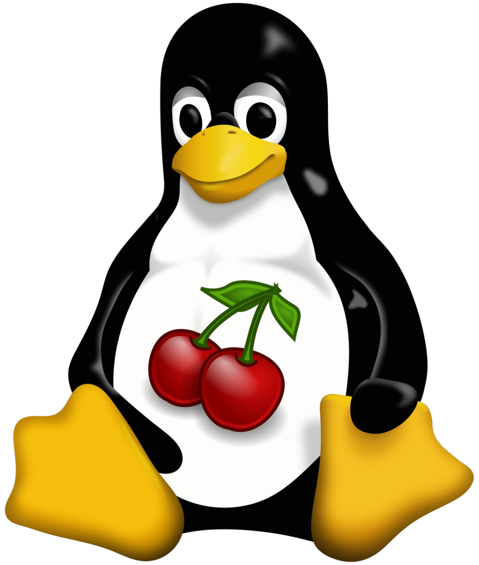
Morello Linux

“Our Motto”

Morello Linux – *“Our Motto”*

Let Linux developers focus on their capability based usecase.

Meaning: Enable Linux developers to develop/port their Linux applications on the Morello architecture and researchers to target security and performance investigations in userspace.

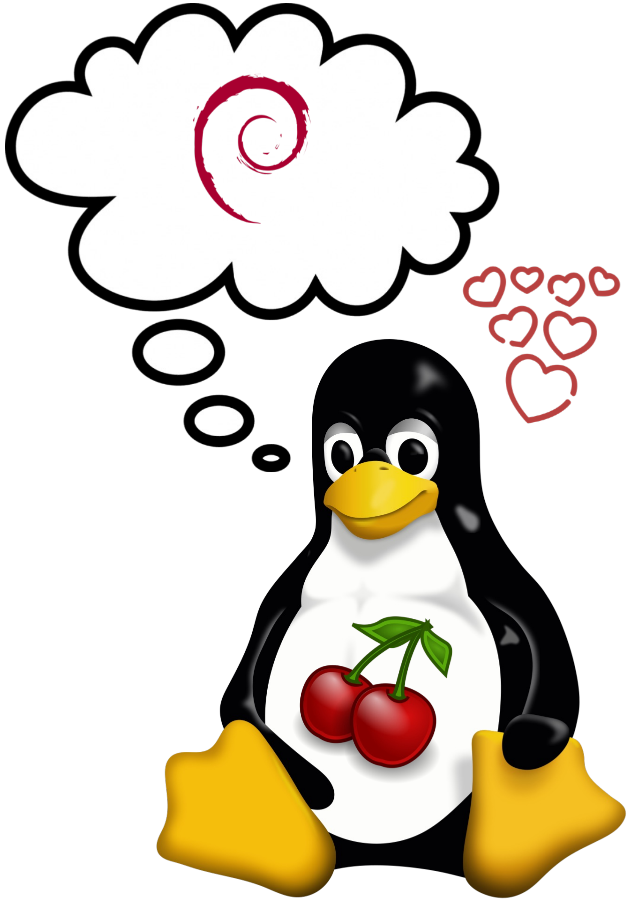


Morello Linux

Status of Morello Linux

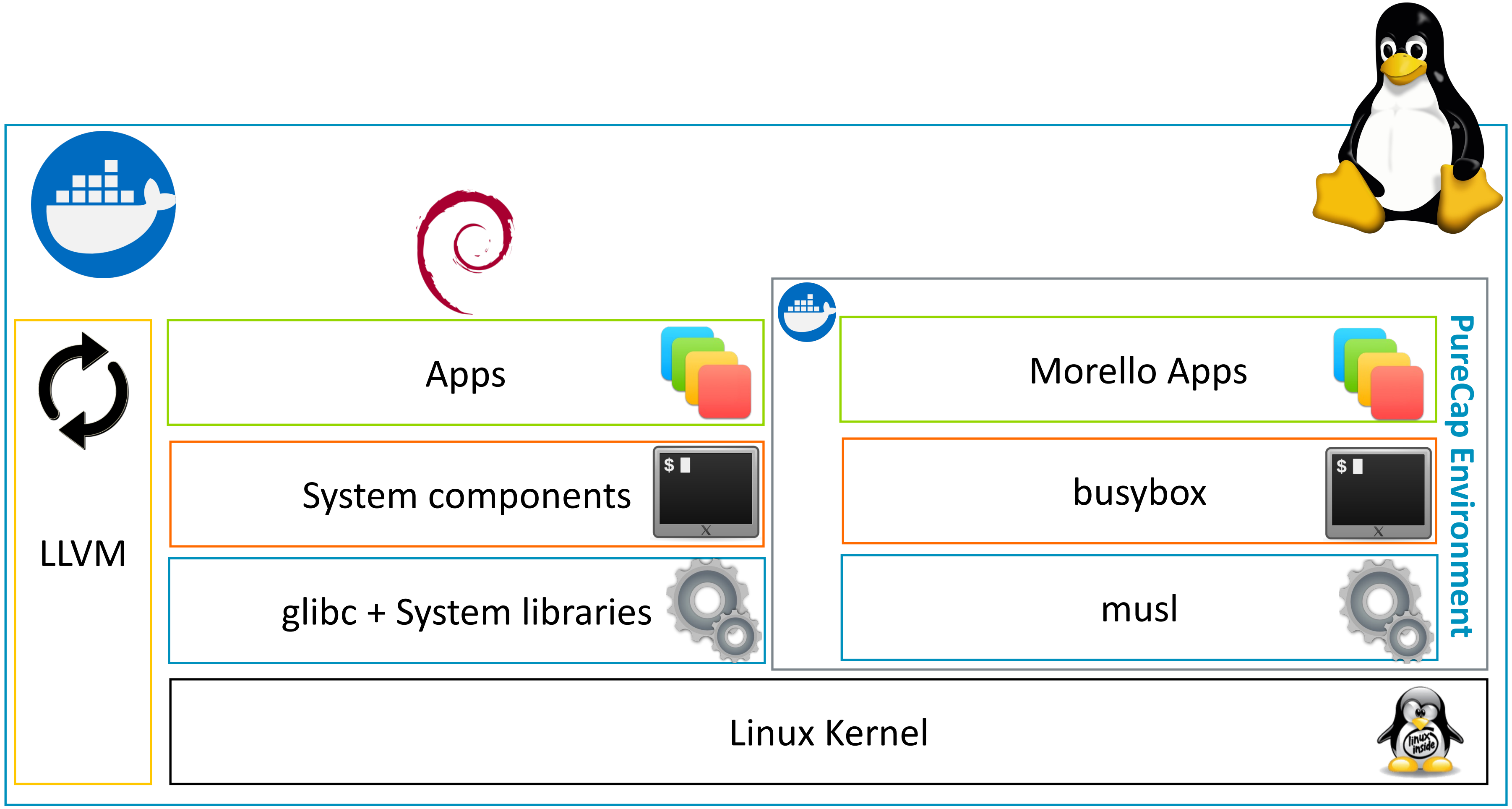
Morello Linux

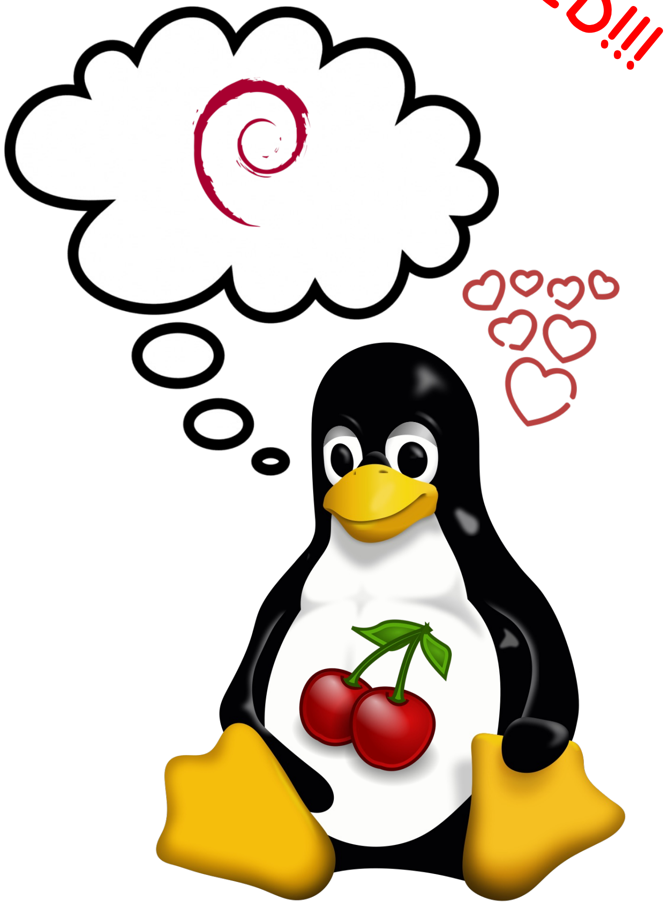
HELP WANTED!!!



Morello Linux – Hybrid Software Stack

HELP WANTED!!!





Morello Linux – Initial Release in April 2023

Morello SDK

In less than 10 minutes you should be able to setup a docker container with everything you need to build an application for Morello.

- Documentation: https://sdk.morello-project.org/
- Code repository: https://git.morello-project.org/morello/morello-sdk

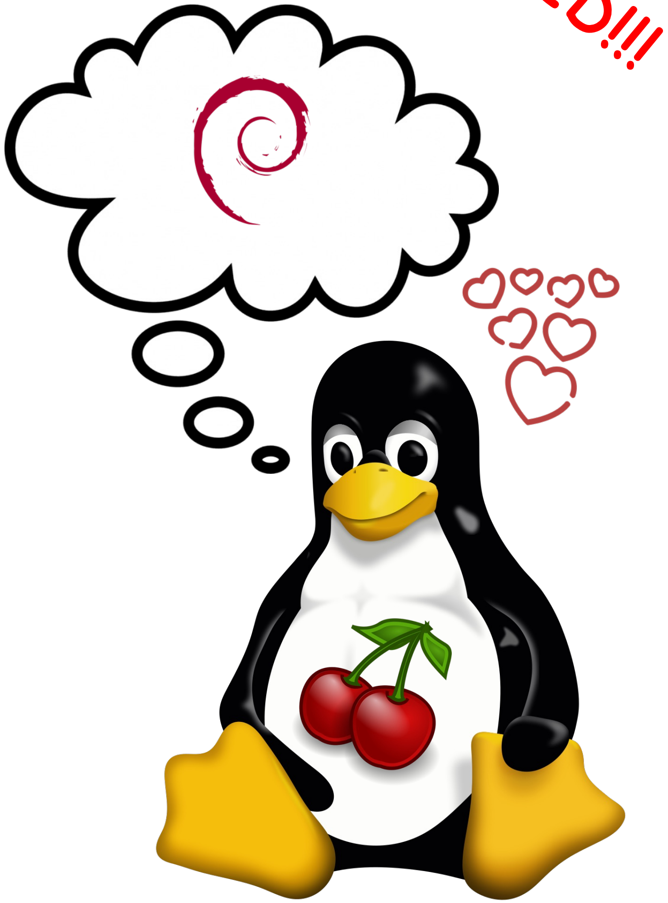
Morello Linux

In less than 10 minutes you should be able to setup a docker container with everything you need to build and boot into a Morello Debian environment.

- Documentation: https://linux.morello-project.org/
- Code repository: https://git.morello-project.org/morello/morello-linux

Note: The documentation covers the instructions for Linux but if you know what you are doing and are familiar with docker no one stops you from running our solution on Windows or Mac.

HELP WANTED!!!



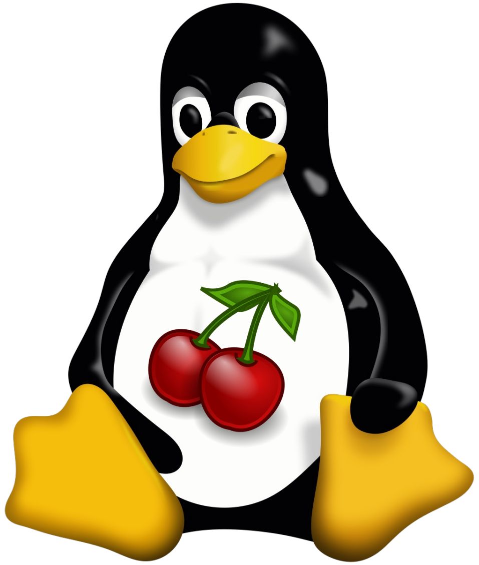
Morello Linux

Integration Drop 1.8 – April 2024

Morello Linux – Release 1.8 (April 2024)

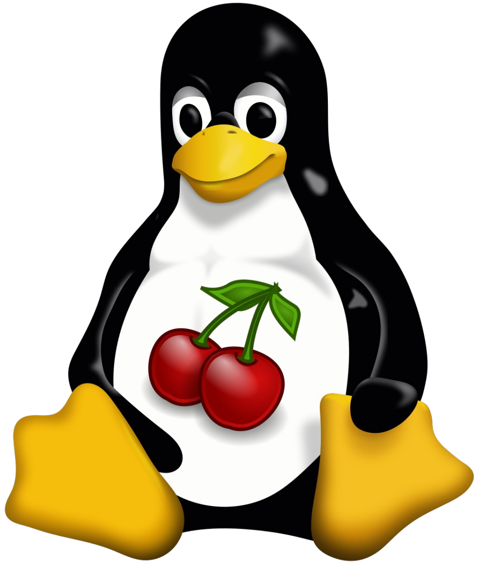
Highlights:

- Updated Linux Kernel ABI.
- More frequent Linux Kernel Binary Updates.
- mcli tool to install more conveniently the Morello SDK.
- New version for musl and LLVM with bug fixes and new features.
- Improved coverage of the LTP test environment.



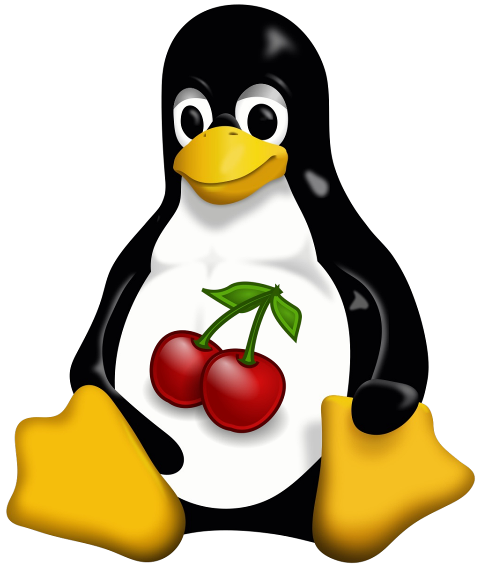
Morello Linux – Updates of Linux Kernel ABI (April 2024)

- Restrict most of the initial capabilities provided by the kernel.
- Implement PCuABI address space management and reservations.
- Hardening (sandboxing) of eBPF to mitigate verifier bypass vulnerabilities that result in arbitrary kernel read/writes
  - Running JIT'd eBPF in a hybrid compartment using Restricted/Executive mode for domain transitions.
  - Exploits resulting in arbitrary kernel read/write instead become kernel Oops due to capability fault accessing out of bounds memory.
- Support KVM for Morello: basic enablement, targeting at adding support for Morello at EL2:
  - Add support for HW attributes, accessing, saving and restoring capability registers.
  - Introduce compat for KVM to allow running aarch64 guests, no official support for purecap guests.



Morello Linux – Updates of Linux Kernel ABI (April 2024)

- DRM compat arm64 fully works.
- DRM purecap ABI partially implemented and tested.
- Userspace graphics stack built up to kmscube.
- Fix various issues (kernel, LTP, Musl).
- Update Morello LTP fork to 20230929 upstream tag.



Morello Linux

What’s Next?

Opportunities for Ecosystem Research

Morello Linux – Future opportunities for the Ecosystem Research

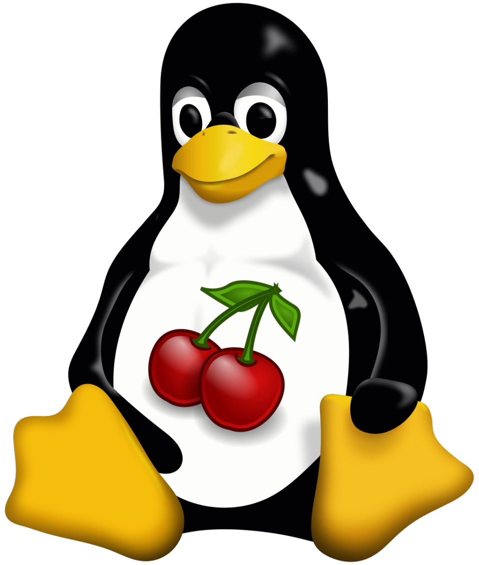
HELP WANTED!!!

Goal: Identify areas where we can leverage Morello's Security capabilities to improve performances.

We are currently actively working on two areas that seem worth investigation (to begin with):

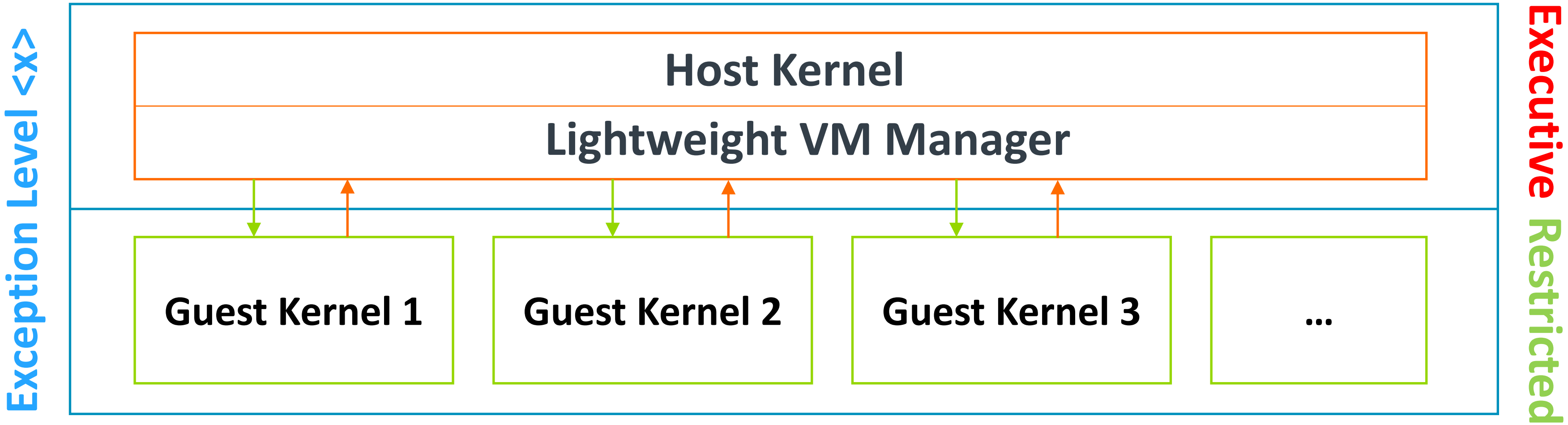
- Lightweight VMs
- eBPF JIT engine

Note: The purpose of our activities is to identify opportunities for future ecosystem research. We will do our part, but we recognize that without the help coming from the community we will not be able to deliver on these areas.

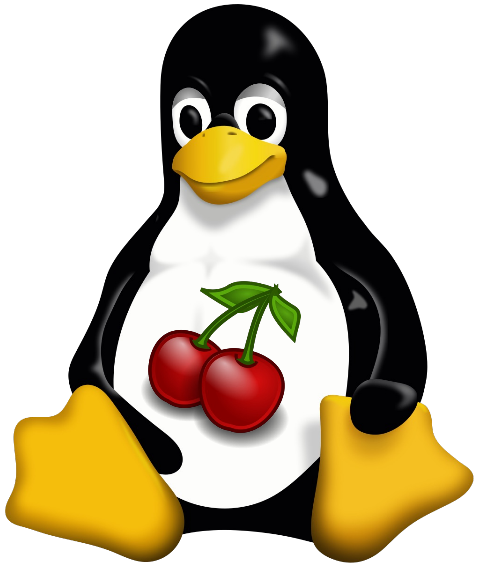


Morello Linux – Lightweight VMs (1/2)

HELP WANTED!!!



Note: ∃ x/x ∈ {1,2}



Morello Linux – Lightweight VMs (2/2)

HELP WANTED!!!

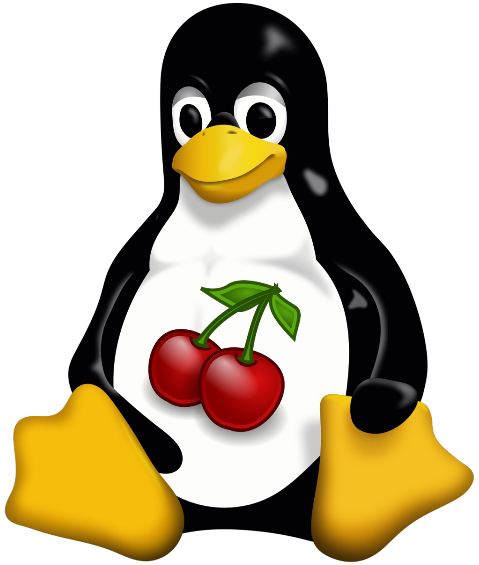
The idea is to leverage Executive and Restricted to narrow down necessary context switching.

We know that this is not achievable with the current version of Morello architecture.

The purpose of the investigation is to find what is missing in the Morello Architecture to make this use-case possible.

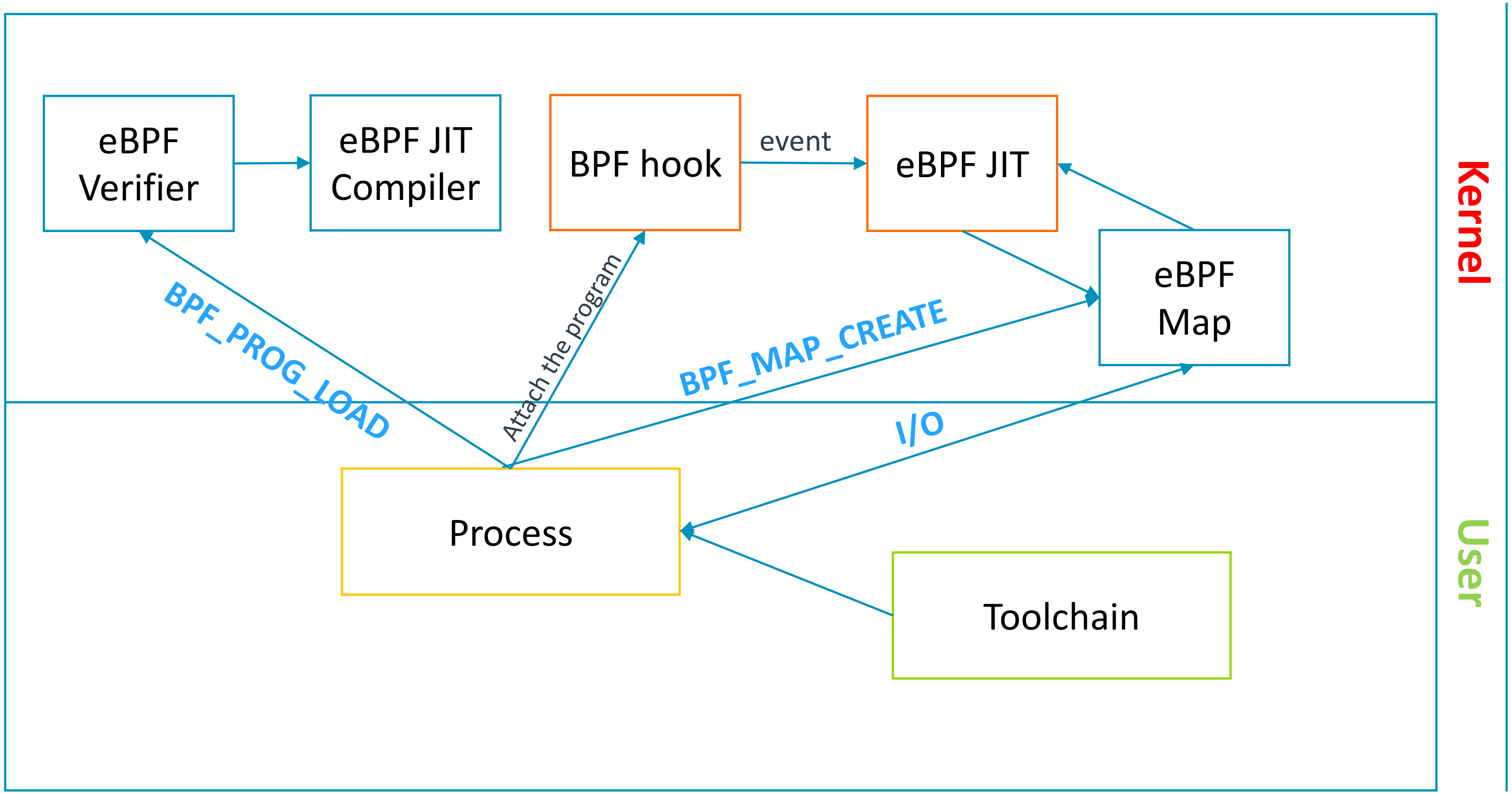
In doing so, with the help of the community, we aim to use KVM as a reference and to try as a long-term goal to emulate (where possible) the parts of the architecture that are missing.

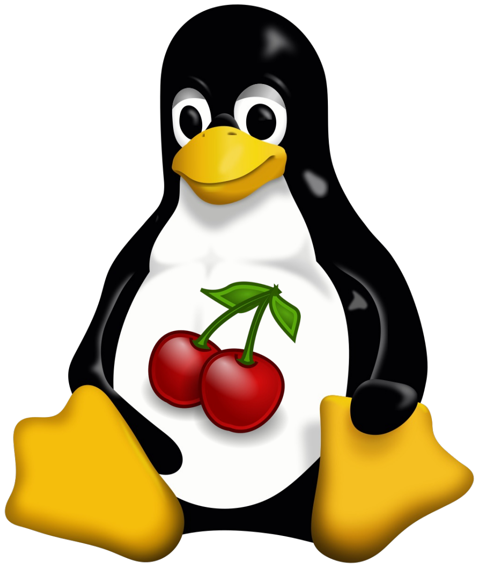
Status: We started the investigation at the end of June 2023. If you are interested in the topic, it is the right time to join the effort.



Morello Linux – eBPF

HELP WANTED!!!





Morello Linux – July 2021: Discovered a vulnerability, CVE-2021-3490

HELP WANTED!!!

There have been many CVEs that trick the eBPF verifier into loading and running unsafe code [1].

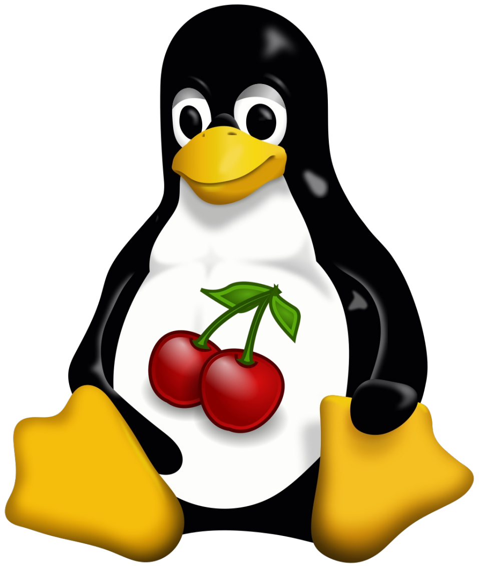
e.g. **CVE-2021-3490** [0]

eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the eBPF verifier did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution.

Our approach: with the help of the community, we aim to sandbox JIT'd eBPF execution with a hybrid compartment. This will allow eBPF to be used more safely, in new ways.

Lightweight isolation of JIT'd code from kernel memory means any exploits previously resulting in arbitrary kernel memory read/writes are prevented at runtime with capability faults.

Status: RFC patches are out on the list. If you are interested in eBPF this is an opportunity to help to enhance security in this area.



[0] https://chomp.ie/Blog+Posts/Kernel+Pwning+with+eBPF+-+a+Love+Story

[1] https://security.googleblog.com/2023/05/introducing-new-way-to-buzz-for-ebpf.html

Morello Linux

Our Community

Morello Linux – Mailing List

- The mailing list is considered as the center of the community life.
- Linux Kernel Mailing List: linux-morello@op-lists.linaro.org
- Morello-flavored Linux Test Project (LTP) discussions: linux-morello-ltp@op-lists.linaro.org
- Morello Linux Kernel CI Reports: linux-morello-ci@op-lists.linaro.org
- Morello Linux Distros Discussions: linux-morello-distros@op-lists.linaro.org

Morello Linux – Thank you!

✉ vincenzo.frascino@arm.com

https://twitter.com/fvincenzo

Thank You

Danke

Merci

谢谢

ありがとう

Gracias

Kiitos

감사합니다

धन्यवाद

شكرًا

ধন্যবাদ

תודה