INSTITUTO DE COMPUTAÇÃO

UNICAMP

Hands-on exercise (Mini course)

Process Confinement and Resource Limitation in IoT Devices with Embedded Linux

William Lima Reiznautt

Institute of Computing, University of Campinas

mail: william@unicamp.br / https://www.ic.unicamp.br

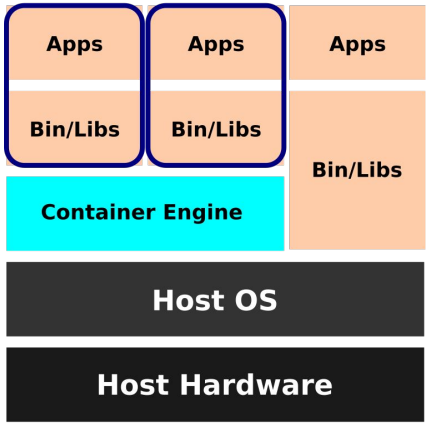
H.IAAC | HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

Hands-on goals

INSTITUTO DE COMPUTAÇÃO

UNICAMP

- Understand how the Linux kernel controls resources
- Confine processes without Docker
- See the foundation of modern containers in practice



Today we will manually build a ‘container’ using only the Linux kernel.

Hands-on exercise (Mini course)
Process Confinement and Resource Limitation in IoT Devices with Embedded Linux

H.IAAC | HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

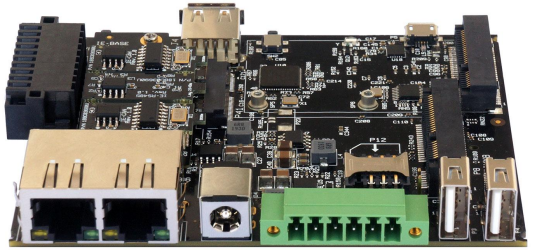
What Are We Simulating?

INSTITUTO DE COMPUTAÇÃO

UNICAMP

Environment

- Embedded Linux with ARM64 IoT device (simulated)
- Limited CPU and memory (small device)
- Real Linux kernel features



This is what runs inside gateways, SBCs, and industrial devices.

H.IAAC | HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

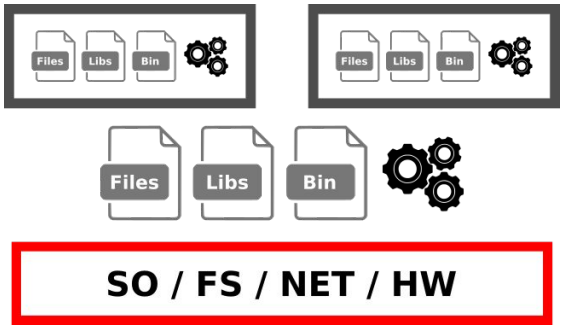
Linux Kernel Building Blocks

INSTITUTO DE COMPUTAÇÃO

UNICAMP

Three key kernel mechanisms

- **cgroups** → limit CPU and memory (others I/O)
- **chroot** → restrict filesystem view
- **namespaces** → isolate network and processes



This is the base of Docker isolation. These features are Kernel Linux.

cgroups: Resource Control

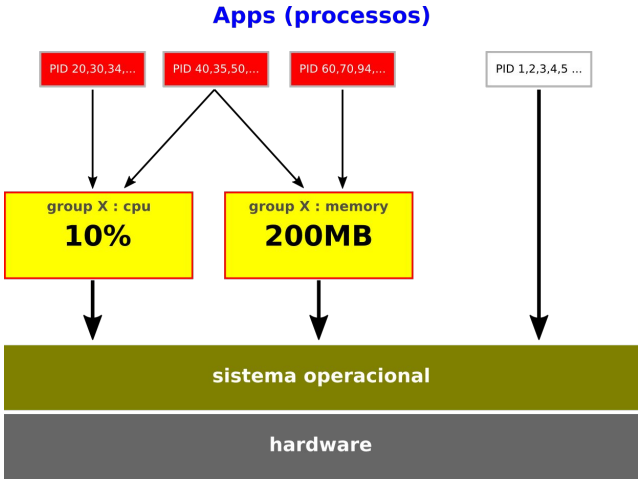
INSTITUTO DE COMPUTAÇÃO

UNICAMP

What we do in the hands-on

- Create a CPU cgroup
- Limit a process to 20% of one core
- Test with a CPU-hungry process
- Repeat with memory limits

Here the kernel enforces resource limits at runtime.



H.IAAC HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

chroot: Filesystem Isolation

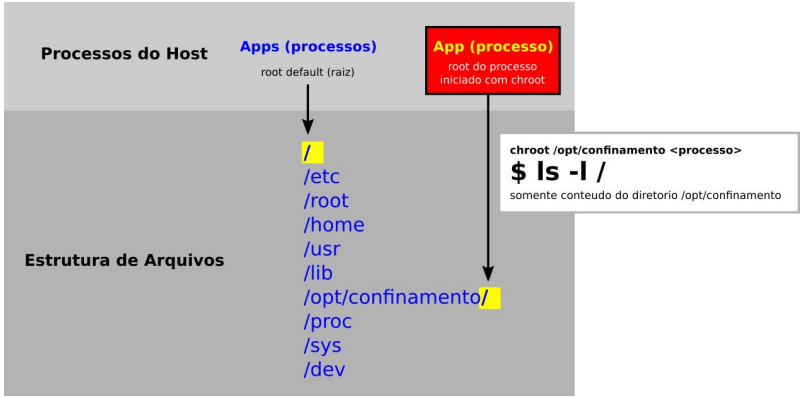
INSTITUTO DE COMPUTAÇÃO

UNICAMP

What chroot does

- Changes the root directory of a process
- The process sees a different filesystem
- Old, simple, and powerful mechanism

The process thinks it is alone, but it isn’t.



Hands-on exercise (Mini course)
Process Confinement and Resource Limitation in IoT Devices with Embedded Linux

H.IAAC HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

Network Namespaces

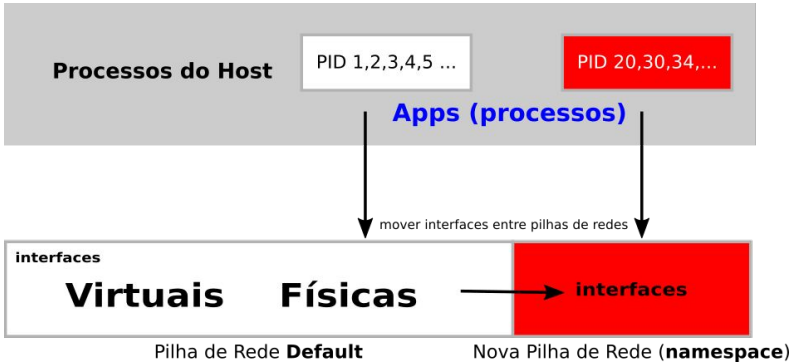
INSTITUTO DE COMPUTAÇÃO

UNICAMP

What we isolate

- Network interfaces
- IP addresses, routes, firewall and ports
- Independent TCP/IP stack

Each process can have its own network.



Others namespaces to isolate (IPC, User, UTC, Mount, PID, Time)

https://man7.org/linux/man-pages/man7/namespaces.7.html

Hands-on exercise (Mini course)
Process Confinement and Resource Limitation in IoT Devices with Embedded Linux

H.IAAC HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

Putting It All Together

INSTITUTO DE COMPUTAÇÃO

UNICAMP

Final combination

- cgroups → CPU and memory limits
  (used to isolate resource usage and reduce overall resource and energy consumption)
- chroot → filesystem confinement
- network namespaces → isolated networking

Result

- A confined process
- Behavior similar to a Docker container without Docker Engine

Containers are a natural consequence of the Linux kernel.

H.IAAC | HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

Practical IoT Example: Why Resource Limitation Matters

Scenario:
- Embedded IoT gateway running multiple services
- Sensor data collection, web interface, cloud communication

Problem:
- A faulty or malicious process can consume all CPU or memory
- Entire device becomes unstable or unresponsive

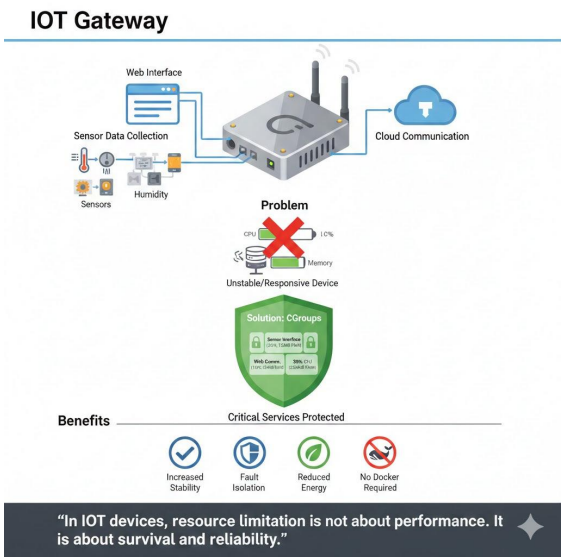
Solution:
- Use cgroups to limit CPU and memory per process
- Critical services remain protected

Benefits:
- Increased system stability
- Fault isolation
- Reduced energy consumption
- No Docker required

Hands-on exercise (Mini course)
Process Confinement and Resource Limitation in IoT Devices with Embedded Linux

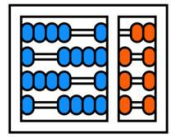
INSTITUTO DE COMPUTAÇÃO

UNICAMP



H.IAAC | HUB DE INTELIGÊNCIA ARTIFICIAL E ARQUITETURAS COGNITIVAS

Hands-On Exercise



Step-by-Step Tutorial:

https://www.ic.unicamp.br/~william/3rd-iot-panama-26/

- Access your virtual machine for the hands-on session (with your number)
- Simulated Embedded Linux ARM environment
- Apply process isolation using practical examples

The tutorial is available in English, Spanish, and Portuguese for your convenience.