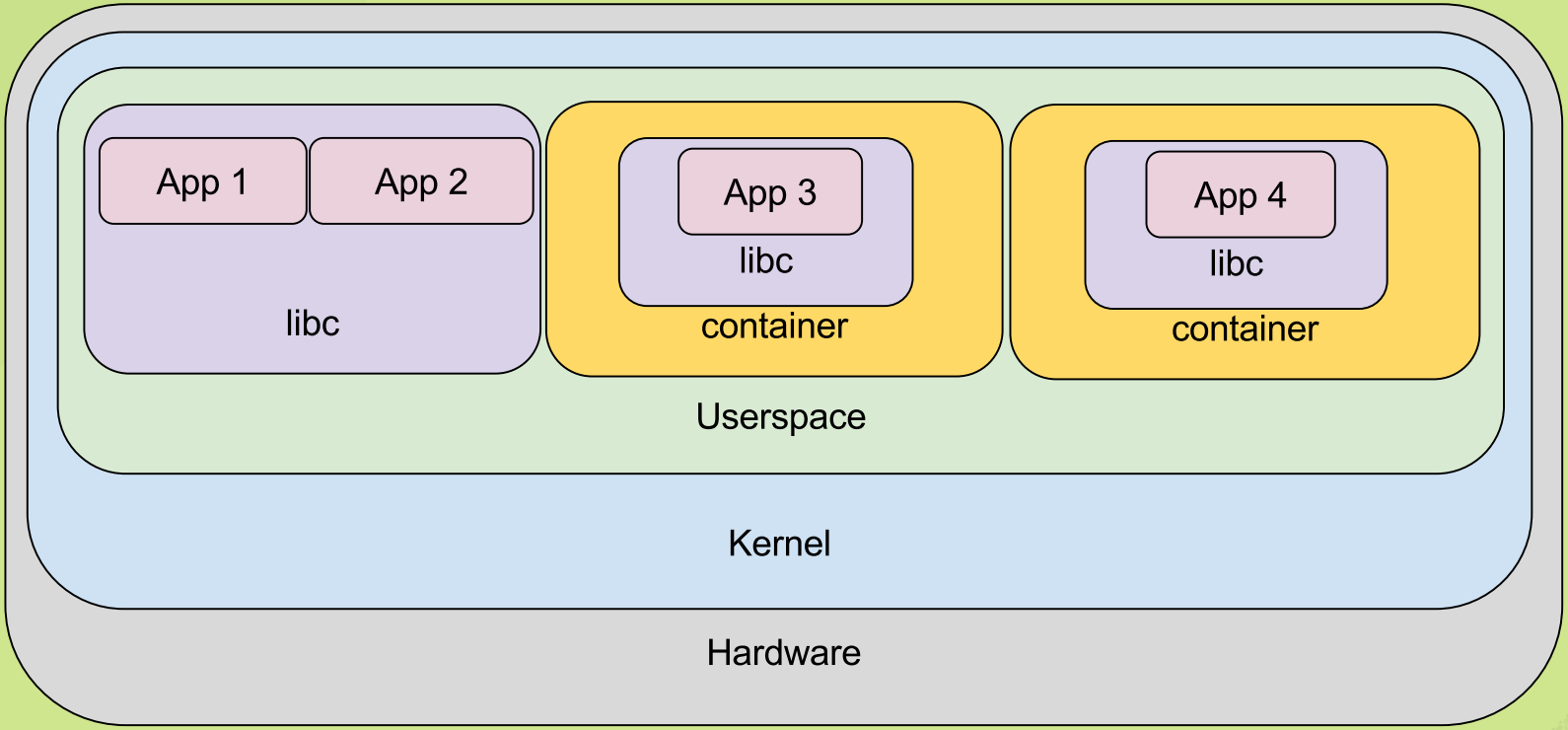
CONTAINERS, COMPUTING AND CHANGE

Vincent Batts @vbatts

```
$> finger $(whoami)
Login: vbatts                           Name: Vincent Batts
Directory: /home/vbatts                 Shell: /bin/bash
Such mail.
Plan:
OHMAN
$> id -Gn
devel opencontainers docker appc redhat golang slackware
```

CONTAINERS

(Cite: The Internet)


App 1
App 2
libc
App 3
libc
container
App 4
libc
container
Userspace
Kernel
Hardware

CONTAINERS:

CONTAINERS:

Share the host's kernel

CONTAINERS:

Share the host's kernel

Crashes and Exploits alike

CONTAINERS:

Share the host's kernel

Crashes and Exploits alike

virtualizing by "namespacing" kernel resources and concepts

CONTAINERS:

Share the host's kernel

Crashes and Exploits alike

virtualizing by "namespacing" kernel resources and concepts

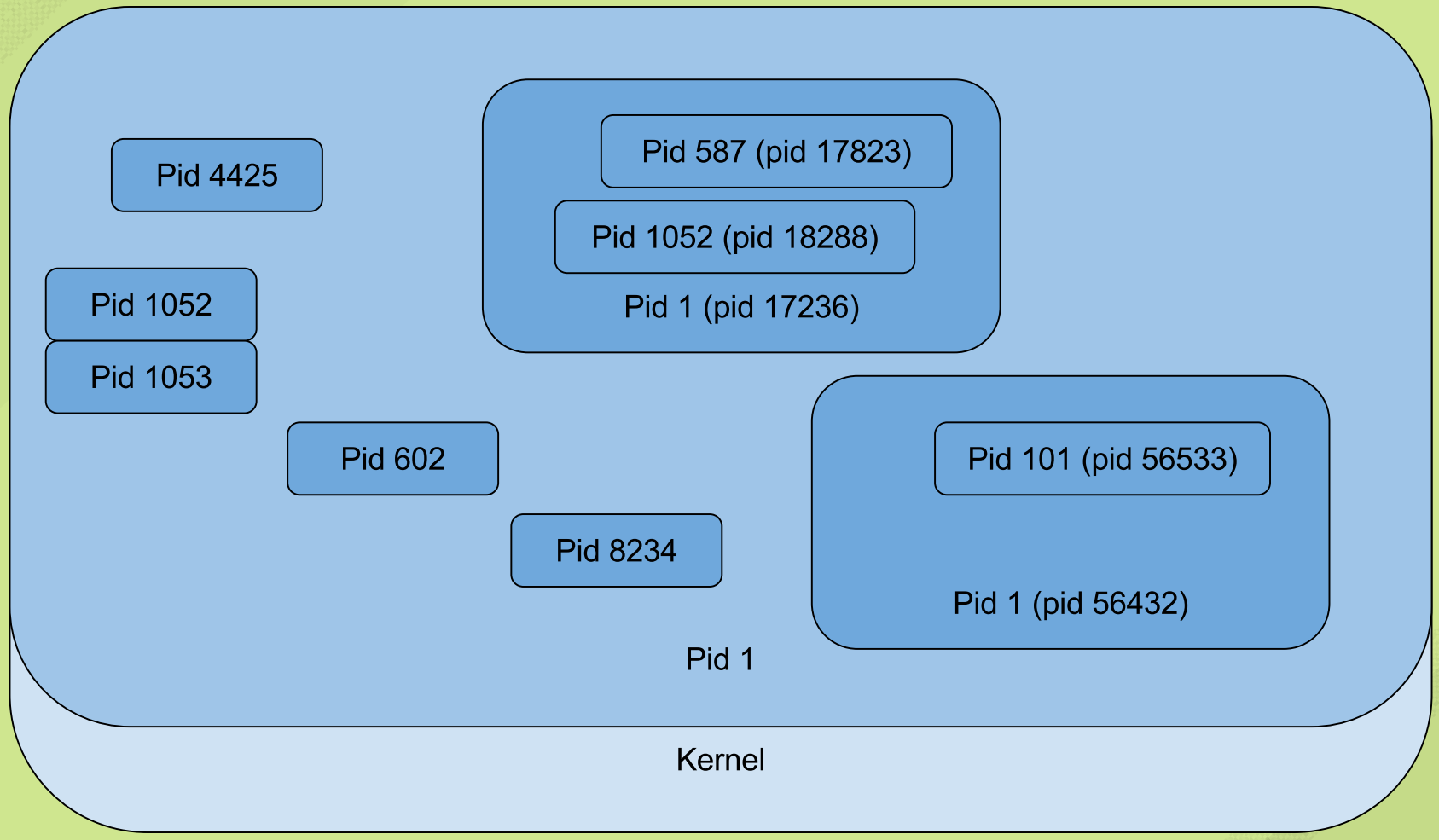
Isolation by control groups, syscall filtering, and Linux Security Modules (SELinux, apparmor, etc.)

KERNEL NAMESPACES:

unshare() docs

- mount
- IPC (message queues, semaphores, shm)
- UTS (hostname)
- network
- PID
- cgroup
- user

KERNEL NAMESPACES: PID



CONTAINER RUNTIME STANDARDS

OpenContainer Initiative Runtime Specification

```
$> runc spec
$> less config.json
{
        "ociVersion": "1.0.0-rc5",
        "platform": {
                "os": "linux",
                "arch": "amd64"
        },
        "process": {
                "terminal": true,
...
```

Using runc

CONTAINER DISTRIBUTION

CONTAINER DISTRIBUTION

Root ('/') File System

CONTAINER DISTRIBUTION

Root ('/') File System

Approaches:

- Tar Archive
- Raw Image
- rsync
- ostree

CONTAINER DISTRIBUTION

```
$ skopeo copy docker://opensuse/amd64:42.2 oci:opensuse:latest
Getting image source signatures
Copying blob sha256:b0d17859d0e6c32023637374cc2a58223f013758bf13b5b390e00f1c89556cb8
 47.09 MB / 47.09 MB [============================================================]
Copying config sha256:402d70d449419de6963c694b69af418d35a026ad14159e93da8ef9973db21605
 0 B / 805 B [--------------------------------------------------------------------]
Writing manifest to image destination
Storing signatures
$ find ~/opensuse -type f
/home/vbatts/opensuse/blobs/sha256/ca2b806433c495ede5114aec2ffd567b43f084c60774346214b610f8ba0b830
/home/vbatts/opensuse/blobs/sha256/402d70d449419de6963c694b69af418d35a026ad14159e93da8ef9973db2160
/home/vbatts/opensuse/blobs/sha256/b0d17859d0e6c32023637374cc2a58223f013758bf13b5b390e00f1c89556cb
/home/vbatts/opensuse/refs/latest
/home/vbatts/opensuse/oci-layout
```

tools like:

- projectatomic/skopeo
- jessfraz/riddler
- openSUSE/umoci
- opencontainers/image-tools
- opencontainers/runtime-tools

CONTAINER DISTRIBUTION

Distributable formats (see Open Container Initiative)

```
$ skopeo copy docker://opensuse/amd64:42.2 oci:opensuse:latest
Getting image source signatures
Copying blob sha256:b0d17859d0e6c32023637374cc2a58223f013758bf13b5b390e00f1c89556cb8
 47.09 MB / 47.09 MB [============================================================]
Copying config sha256:402d70d449419de6963c694b69af418d35a026ad14159e93da8ef9973db21605
 0 B / 805 B [--------------------------------------------------------------------]
Writing manifest to image destination
Storing signatures
$ find ~/opensuse -type f
/home/vbatts/opensuse/blobs/sha256/ca2b806433c495ede5114aec2ffd567b43f084c60774346214b610f8ba0b830
/home/vbatts/opensuse/blobs/sha256/402d70d449419de6963c694b69af418d35a026ad14159e93da8ef9973db2160
/home/vbatts/opensuse/blobs/sha256/b0d17859d0e6c32023637374cc2a58223f013758bf13b5b390e00f1c89556cb
/home/vbatts/opensuse/refs/latest
/home/vbatts/opensuse/oci-layout
```

tools like:

- projectatomic/skopeo
- jessfraz/riddler
- openSUSE/umoci
- opencontainers/image-tools
- opencontainers/runtime-tools

WHAT'S NEXT?

Desktop applications will shape and mold (see flatpak.org)

Get used to not having root privileges (see bubblewrap and bwrap-oci)

Get used to not having capabilities (see System Tap)

WHAT'S NEXT?

WHAT'S NEXT?

Cloud Native application development (see CNCF)

WHAT'S NEXT?

Cloud Native application development (see CNCF)

Rather than only shoving "legacy" code in new boxes

WHAT'S NEXT?

Cloud Native application development (see CNCF)

Rather than only shoving "legacy" code in new boxes

Discoverable APIs (see OpenAPIs)

WHAT'S NEXT?

Cloud Native application development (see CNCF)

Rather than only shoving "legacy" code in new boxes

Discoverable APIs (see OpenAPIs)

"Scheduled" functionality (see OpenShift and Kubernetes)

WHAT'S NEXT?

Cloud Native application development (see CNCF)

Rather than only shoving "legacy" code in new boxes

Discoverable APIs (see OpenAPIs)

"Scheduled" functionality (see OpenShift and Kubernetes)

intercommunication (see gRPC)

WHAT'S NEXT?

Cloud Native application development (see CNCF)

Rather than only shoving "legacy" code in new boxes

Discoverable APIs (see OpenAPIs)

"Scheduled" functionality (see OpenShift and Kubernetes)

intercommunication (see gRPC)

event and metric driven services

CLOUD

(Cite: the internet)

SHAMELESS PLUG

Red Hat is active in this area

(both technology and proximity)

VINCENT BATTS
@VBATTS| VBATTS@REDHAT.COM

THANKS!