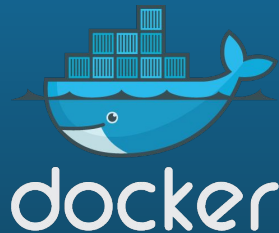


# User Namespaces and Seccomp

## 24 August 2016

Paul Novarese  
Technical Account Manager  
Docker, Inc.  
[pvn@docker.com](mailto:pvn@docker.com)  
@pvn



# Agenda

- Preliminaries
- Container Security Considerations
- Containment
- The User Namespace
- What is Seccomp?
- Demos?

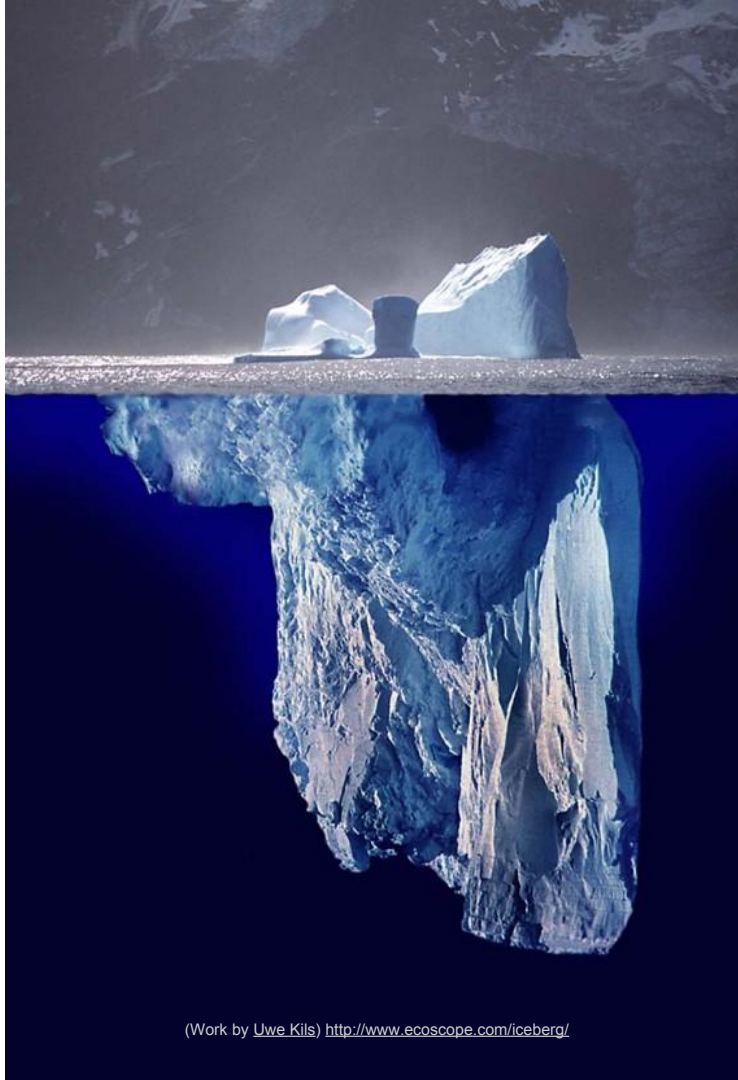
**"CONTAINER"**



**"SECURITY"**

memegenerator.net

# The Iceberg

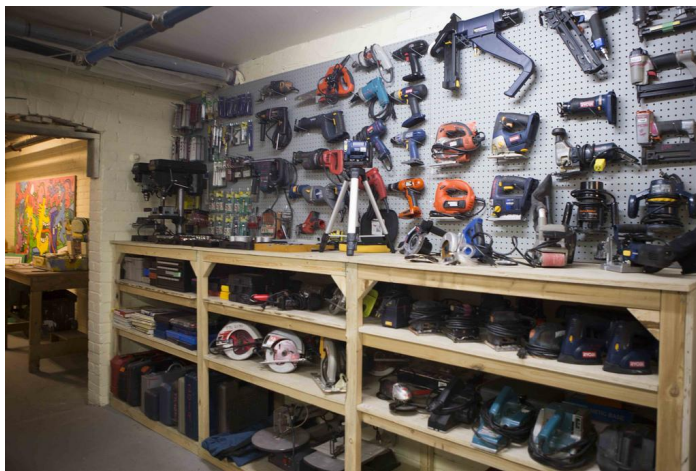


Your code

Your vendor's code

# Containment

- namespaces -> what you can see
- cgroups -> what you can use
- seccomp -> what you can do



# Containment

...applications deployed in containers are **more secure** than applications deployed on the bare OS because **even if a container is cracked** they **greatly limit the damage** of a successful compromise...

<https://www.gartner.com/doc/3375717/secure-docker-containers-operation>



# Namespaces



# Namespaces

```
/ # ps -eo pid,user,args
```

PID	USER	COMMAND
-----	------	---------

1	root	registry serve /etc/docker/registry/config.yml
9	root	sh
13	root	ps -eo pid,user,args

```
/home/docker> ps -eo pid,user,args | egrep "registry|PID"
```

PID	USER	COMMAND
-----	------	---------

1385	root	registry serve /etc/docker/registry/config.yml
------	------	--



# Namespaces

```
/ # ps -eo pid,user,args
```

PID	USER	COMMAND
1	root	registry serve /etc/docker/registry/config.yml
25	root	sh
29	root	ps -eo pid,user,args

```
/home/docker> ps -eo pid,user,args | egrep "registry|PID"
```

PID	USER	COMMAND
748	165536	registry serve /etc/docker/registry/config.yml

## Enabling userns remapping

```
/home/docker> ps ax | grep [d]ockerd  
1425 pts/0    Sl        0:00 dockerd --userns-remap=dockremap
```

```
/home/docker> grep dockremap /etc/passwd  
dockremap:x:100:101:Linux User,,,:/home/dockremap:/bin/false
```

```
/home/docker> cat /etc/subuid  
dockremap:165536:65536
```

# seccomp



# seccomp profiles

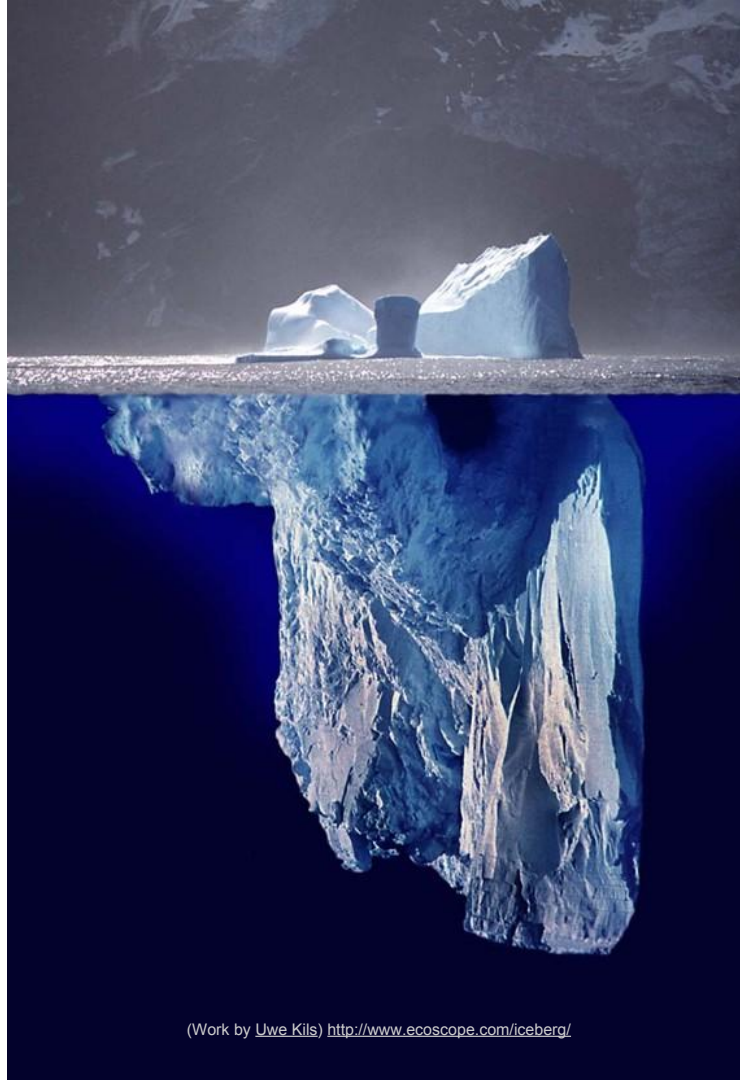
```
{  
  "defaultAction": "SCMP_ACT_ERRNO",  
  "architectures": [  
    "SCMP_ARCH_X86_64",  
    "SCMP_ARCH_X86",  
    "SCMP_ARCH_X32"  
  ],  
  "syscalls": [  
    {  
      "name": "accept",  
      "action": "SCMP_ACT_ALLOW",  
      "args": []  
    },  
    {  
      "name": "accept4",  
      "action": "SCMP_ACT_ALLOW",  
      "args": []  
    },  
  ],  
}
```

# How do I get it?

- You already have it!
- Default profile has been applied to containers since engine 1.10
- For custom profiles, pass **--security-opt** option on the command line.



# The Iceberg (again)



(Work by [Uwe Kils](http://www.ecoscope.com/iceberg/)) <http://www.ecoscope.com/iceberg/>



**STOP TALKING**



**DEMO TIME**

memegenerator.net

**GET EXCITED**



**IT'S DEMO TIME**

memegenerator.net

**TIME FOR A LIVE  
DEMO**



**COULD GO WRONG?**

memegenerator.net

# Demo?

- A DIY demo is available
- <https://twitter.com/pvn> (it will be the pinned tweet)
- If you're reading this in the distant future and I've unpinned the tweet, try this URL instead:

[https://github.com/pvnovarese/workbook/blob/master/pvn\\_containercon\\_users\\_remap\\_lab-2016-08-24.md](https://github.com/pvnovarese/workbook/blob/master/pvn_containercon_users_remap_lab-2016-08-24.md)

# Further Reading, References, etc

- The definitive presentation on userns support:  
[https://events.linuxfoundation.org/sites/events/files/slides/User%20Namespaces%20-%20ContainerCon%202015%20-%202016-9-final\\_0.pdf](https://events.linuxfoundation.org/sites/events/files/slides/User%20Namespaces%20-%20ContainerCon%202015%20-%202016-9-final_0.pdf)
- Default seccomp profile:  
<https://github.com/docker/docker/blob/master/profiles/seccomp/default.json>
- Seccomp docs:  
<https://github.com/docker/docker/blob/master/docs/security/seccomp.md>
- Security non-events:  
<https://docs.docker.com/engine/security/non-events/>
- Gartner Report: How to Secure Docker Containers in Operation  
<https://www.gartner.com/doc/3375717/secure-docker-containers-operation>
- Your Software is Safer in Docker Containers:  
<https://blog.docker.com/2016/08/software-security-docker-containers/>

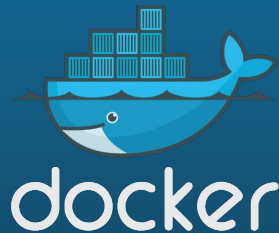
# Booth 41 @ LinuxCon + ContainerCon

Wed Aug 24th

- When the Going gets Tough, Get TUF Going - Riyaz Faizullabhoy (4:35 PM, Frontenac)
- **Toronto Docker Meetup**

Thurs Aug 25th

- Tutorial: Orchestration Containers in Production at Scale with Docker Swarm - Jerome Petazzoni





docker

# Photo credits (all creative commons licensed)

- Iceberg <http://www.ecoscope.com/iceberg/>
- Horses <https://www.flickr.com/photos/arthurtlabar/4275756092/>
- Catan <https://www.flickr.com/photos/bods/6120445526/>
- Workbench <https://www.flickr.com/photos/toollibrary/14427641289>
- memegenerator.net obv