Docker Security

Robert Sugar

July 2015

Docker was NOT Designed for Security

But for ease-of-use and performance

Docker Security Overview

- Docker deamon runs as root
- Containers are isolated
  - Separate namespaces for processes
  - Separate network stack
  - Control Groups (cgroups) limit CPU, I/O, etc.
  - Separate filesystem (with optional mapping to host directories for export/import)

-> there is reasonable protection for applications running inside containers

-> run your apps as non-root inside the container (docker root = host root)

The Docker Group equals root

- Only privilaged users should be allowed to run docker images: **docker group = root**
- Why? – the host is easily rooted from by docker image root

```
docker run -v $PWD:/stuff -t my-docker-image /bin/sh -c \
'cp /bin/sh /stuff && chown root.root /stuff/sh && chmod a+s /stuff/sh’
```

This is by design so. Currently there is no way to run a docker container as a regular user.

Workaround:
use SELinux (which will render directory sharing with –v useless)

Source: reventlov - http://reventlov.com/advisories/using-the-docker-command-to-root-the-host