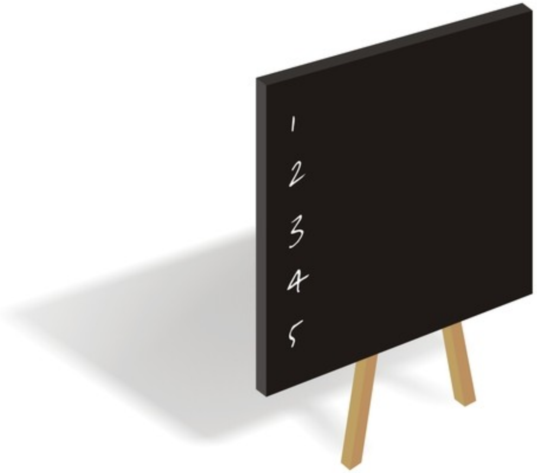
Container Security

with Kata

Udo Seidel

Agenda

- Background
- High level
- Digging deeper
- Take home

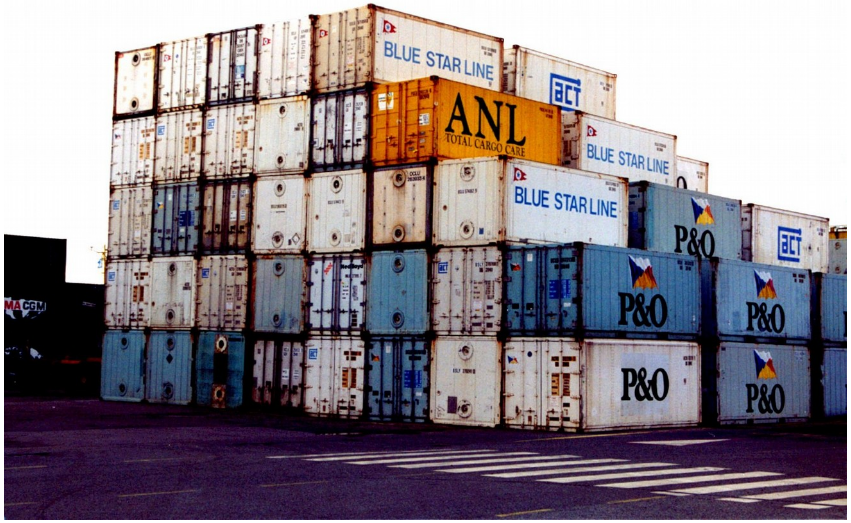


About me

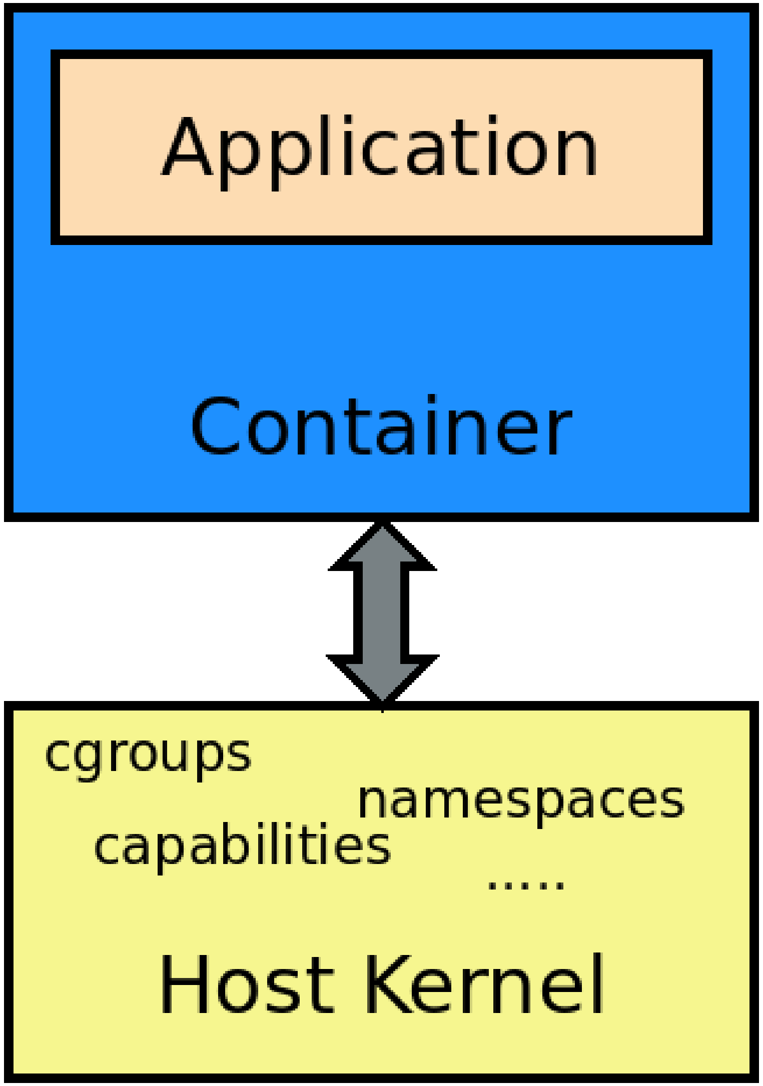
- Teacher of mathematics and physics
- PhD in experimental physics
- Started with Linux/Open Source in 1996
- With Amadeus since 2006
- Before:
  - Linux/UNIX trainer
  - Solution Engineer in HPC and CAx environment
- Now: Architecture & Technical Governance

Containers do not contain

- Has always been the case
- Still true
- Will it ever be fixed?



High level Container



Target of container attacks

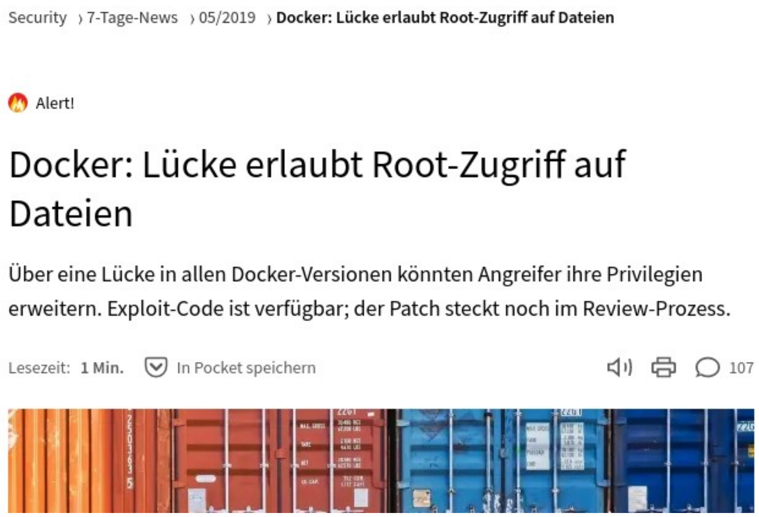
- Host
- Kernel
- Co-running containers
- Other hosts
- ...

What to do?

- Seal containers ultimately
- Secure the host
- All of the above :-)

Sealing of Containers

- Easier said than done
- Not fixed after 6+ years



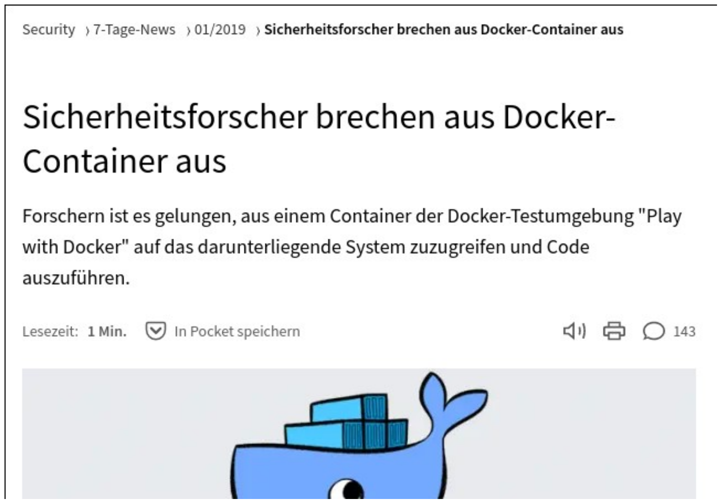
Security › 7-Tage-News › 05/2019 › **Docker: Lücke erlaubt Root-Zugriff auf Dateien**

Alert!

Docker: Lücke erlaubt Root-Zugriff auf Dateien

Über eine Lücke in allen Docker-Versionen könnten Angreifer ihre Privilegien erweitern. Exploit-Code ist verfügbar; der Patch steckt noch im Review-Prozess.

Lesezeit: **1 Min.** In Pocket speichern 107



Security › 7-Tage-News › 01/2019 › **Sicherheitsforscher brechen aus Docker-Container aus**

Sicherheitsforscher brechen aus Docker-Container aus

Forschern ist es gelungen, aus einem Container der Docker-Testumgebung "Play with Docker" auf das darunterliegende System zuzugreifen und Code auszuführen.

Lesezeit: **1 Min.** In Pocket speichern 143

Secure the host

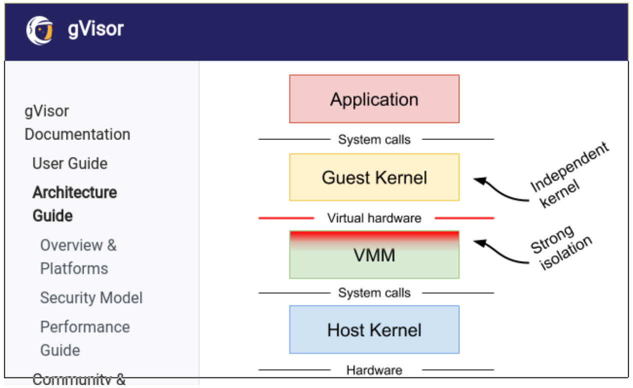
- Hardening
  - Where to cut down further?
  - Risk of breaking things
  - See unikernels and library operating systems
- New security zone
  - Next slide :-)

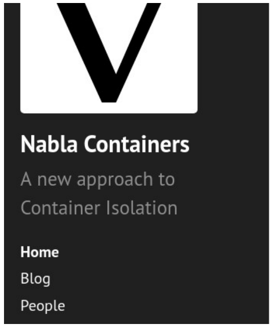
Different approach

- Expect leaks
- Prepare the host
- Prepare the host kernel

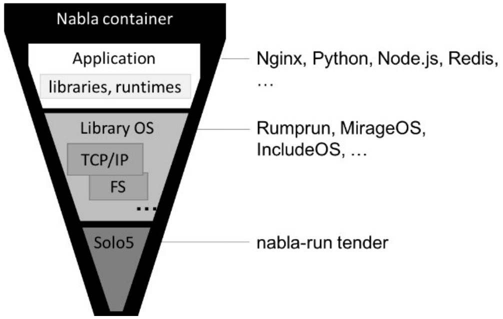
Container DMZ

- Not new → see networks
- Sounds easy at the first glance
- Seems to be “in the air” → Google, IBM




Nabla Containers

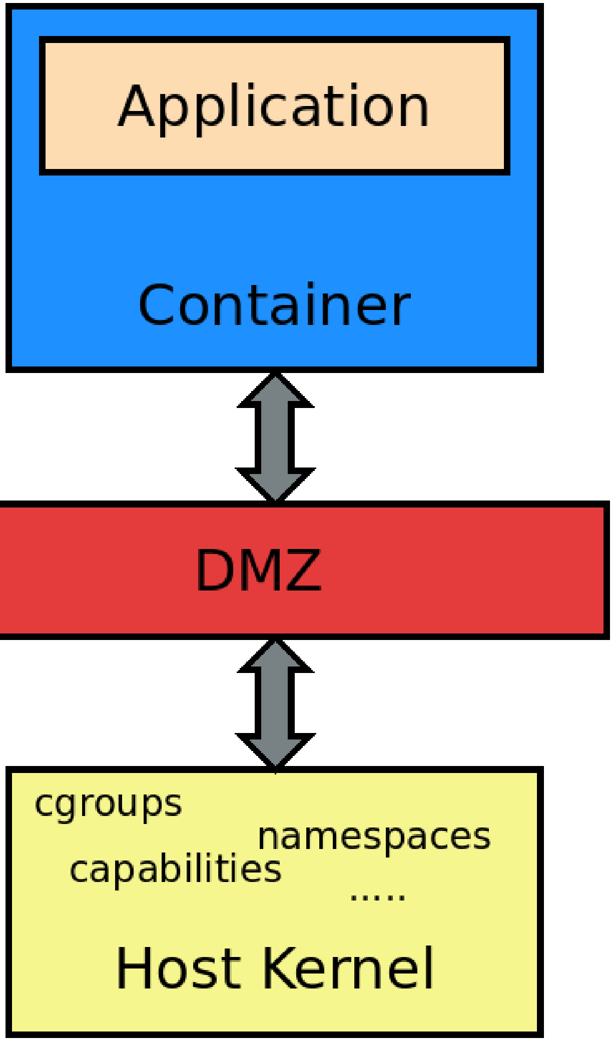
A new approach to Container Isolation



Kata Container

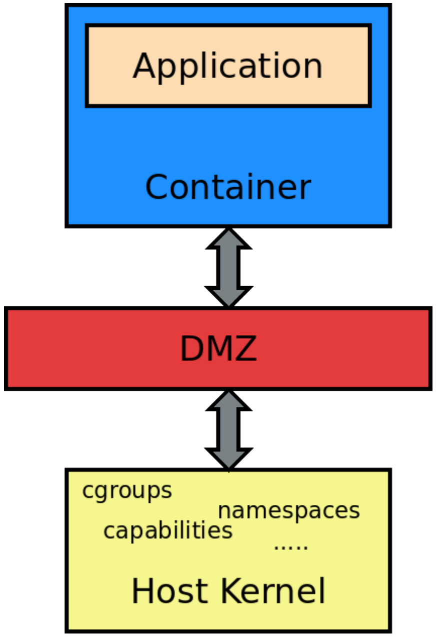
- Name: καταπίστευμα - Trust
- First press release: December 2017
- Merge of
  - Intel Clear Container
  - HyperHQ RunV
- Confirmed project of Openstack Foundation
- License: Apache 2
- Code: Golang
- http://github.com/kata-containers

10000 feet view

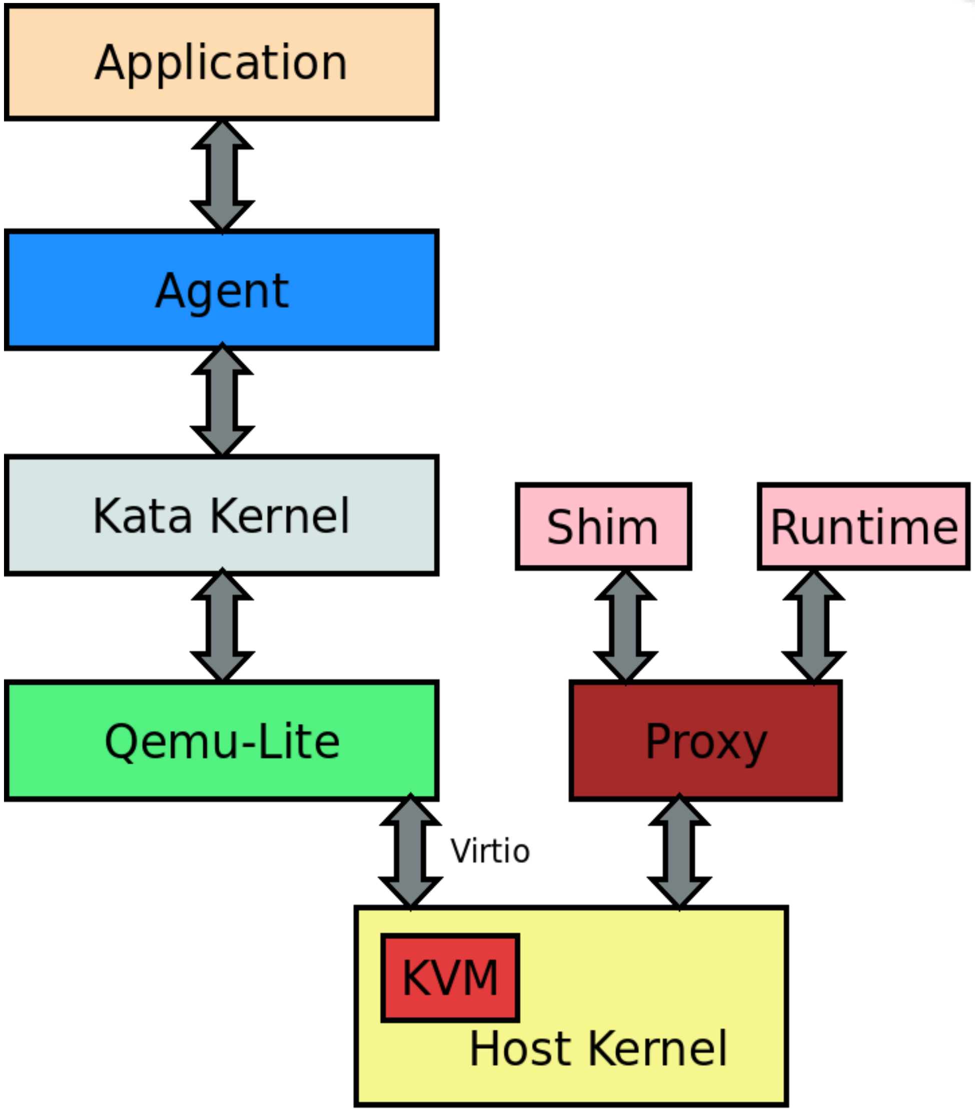


Open questions

- Interaction/API with hypervisor
- Interaction/API with container
  - Docker
  - Kubernetes
  - ….



Detailed architecture



Reality Check

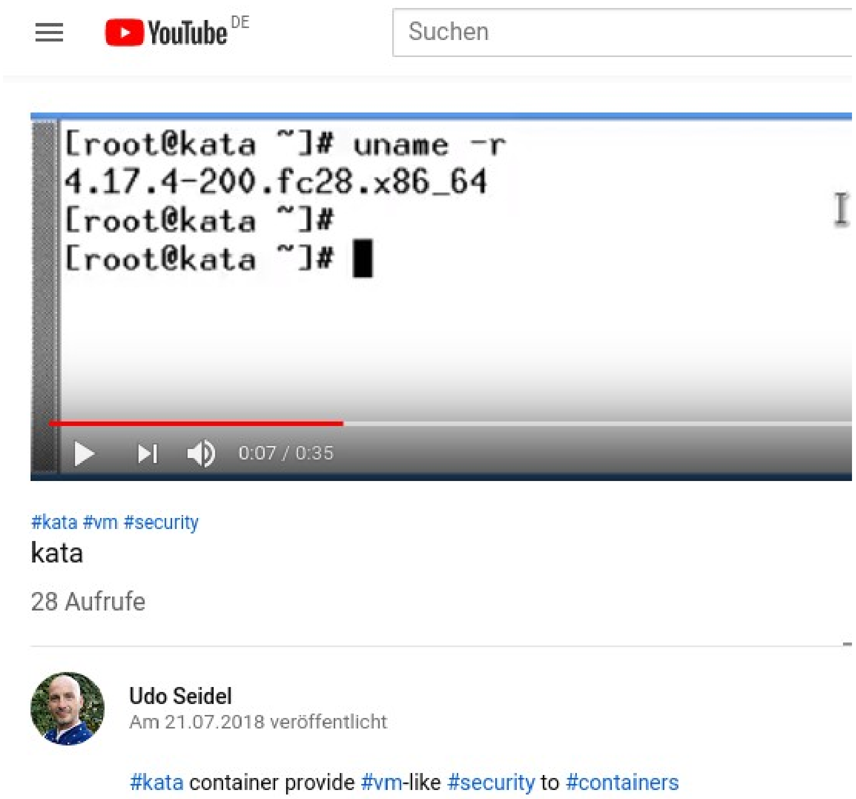
- Packages for famous Linux distributions
- Parallel run with
  - Normal containers
  - gvisor, Nabla, …
- Check-out
  - Clear Linux
  - Qemu .. or Qemu-lite
  - Firecracker (if time permits)

Little Demo :-)

- Knock wood
- Cross your fingers

Demo DR

- https://youtu.be/aLfF6_uFR9Q



```
[root@kata ~]# uname -r
4.17.4-200.fc28.x86_64
[root@kata ~]#
[root@kata ~]# 
```

#kata #vm #security

kata

28 Aufrufe

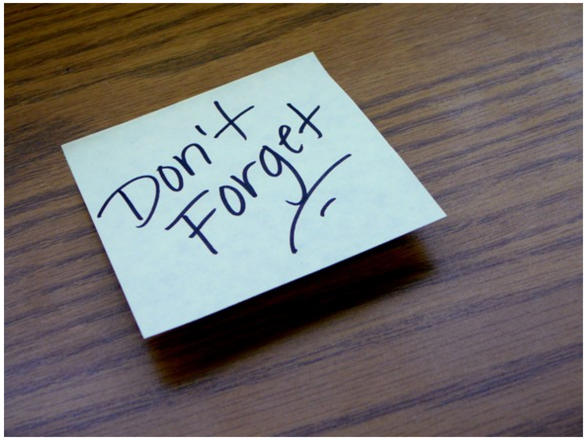
Udo Seidel

Am 21.07.2018 veröffentlicht

#kata container provide #vm-like #security to #containers

Take home

- Container isolation via Type-II hypervisor
- Leveraging existing software/projects
- Quite heavy but manageable
- Hidden “costs” in new layer
- Checkout
  - gVisor
  - Nabla
  - ...



Online resources

- http://katacontainers.io
- http://github.com/kata-containers
- http://clearlinux.org
- http://github.com/qemu-lite
- Internet search :-)