SECURING DATABASES IN CONTAINERS AND SERVICES

By Raghavendra Prabhu

HALL OF FAME/SHAME

DISCOVERED	APR 2014	SEPT 2014	OCT 2014
TYPE	SSL BUG	UNIX SHELL BUG	SSL BUG
AFFECTED SYSTEMS	ANY SYSTEM USING OPENSSL	UNIX, LINUX, OS X, CLIENTS AND SERVERS	ANY CLIENT OR SERVER USING SSL v3
# OF SYSTEMS AFFECTED	MAJORITY OF THE INTERNET	MOST OF THE INTERNET AND INTERNAL SYSTEMS	SMALL % OF THE INTERNET

- Shellshock
- Poodle
- Heartbleed
- RowHammer
- ==> <next one> ==> ?

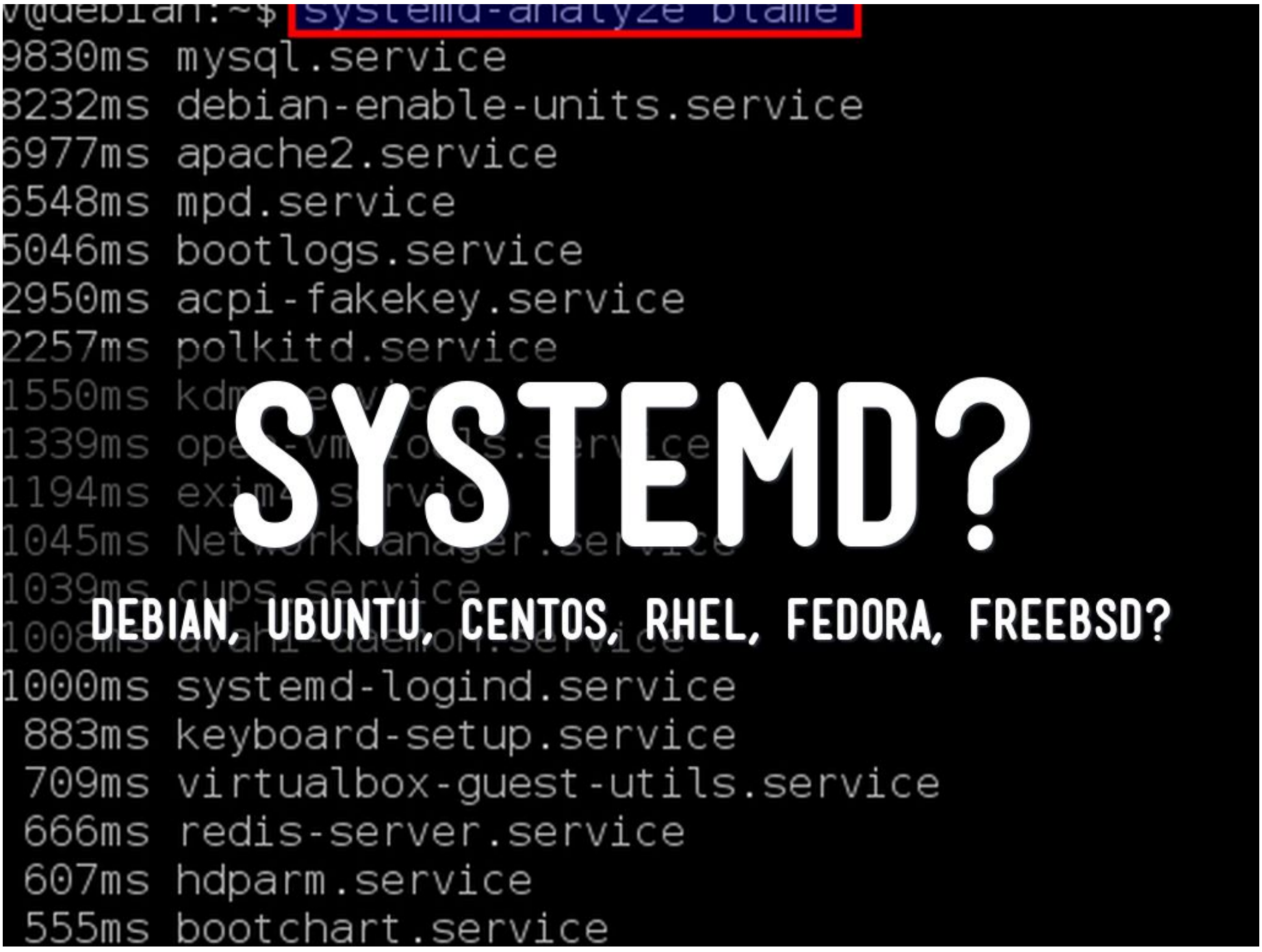
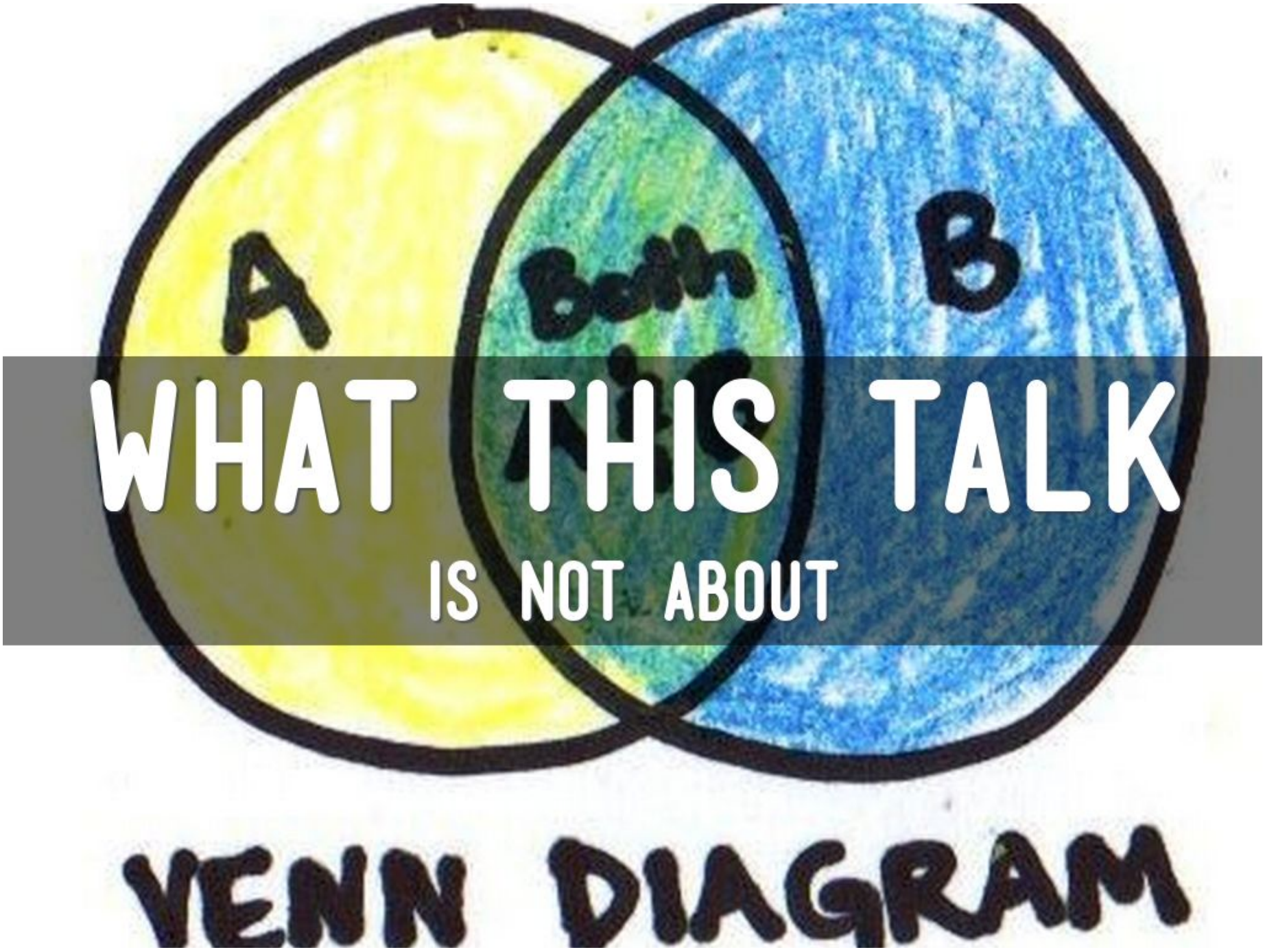
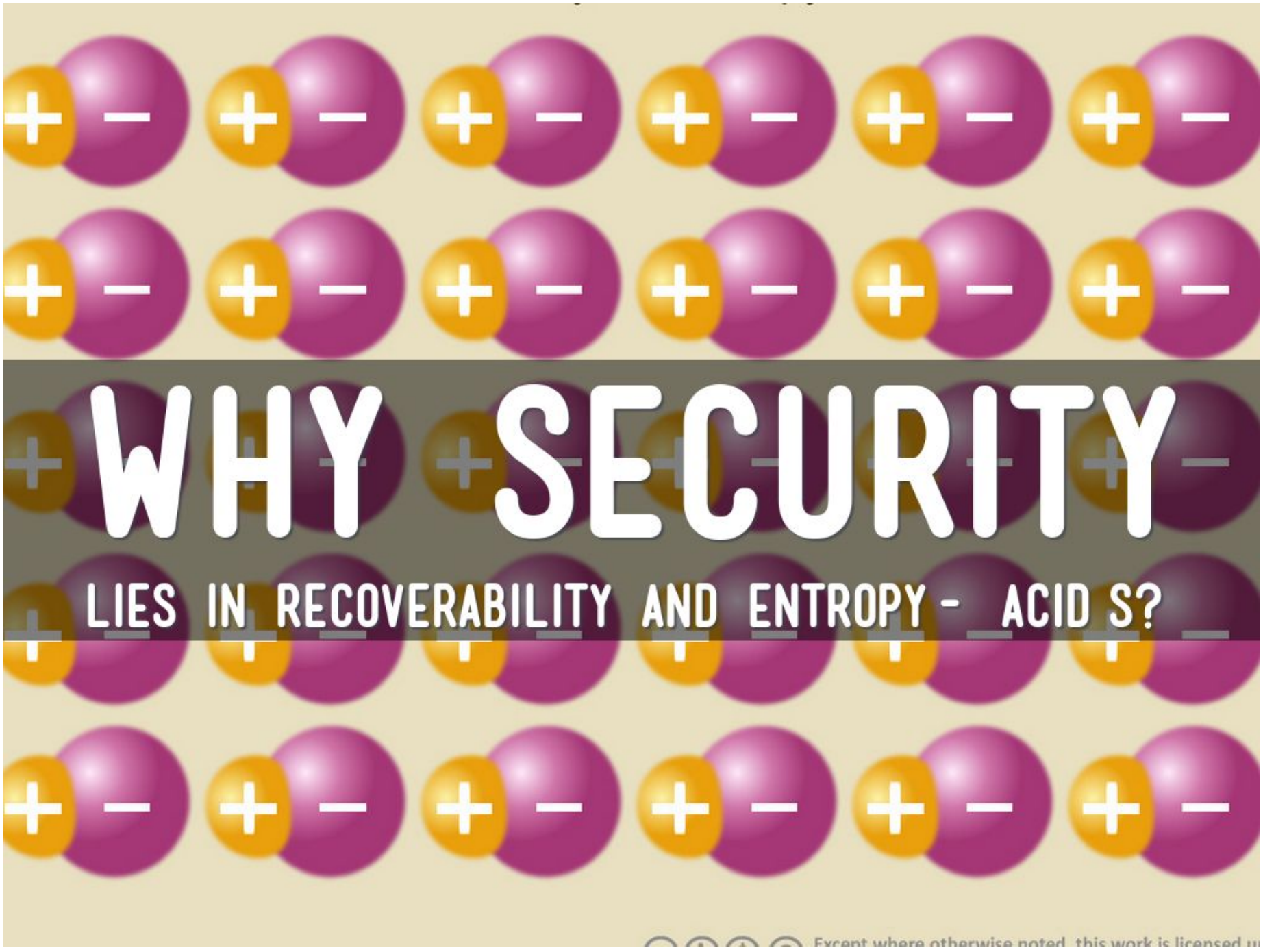


Photo by jdnx



Also, not security from container
but for it!



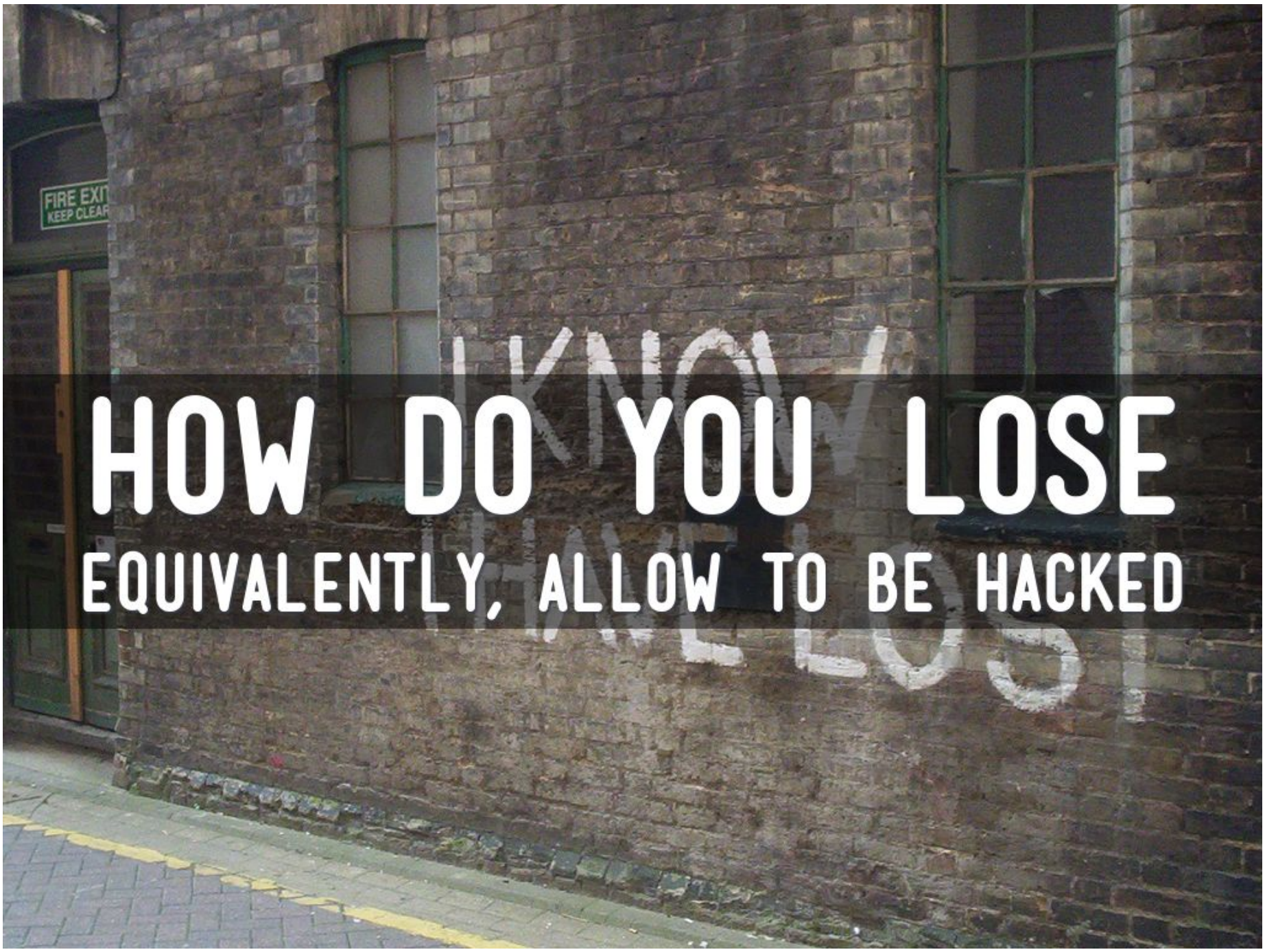
Data is the most valuable entity associated with a system, particularly when it is a sensitive one. Not only are there threats associated with physical access to the box, but also ones where logical access suffices - sql injections etc.

Entropy of data

Deduplication

THINGS TO FOCUS ON

- Malicious Peers/Env (Break-in)
- Malicious Resident (Break-out)
- Containment



is a sensitive one. Not only are there threats associated with physical access to the box, but also ones where logical access suffices - sql injections etc.

Vulnerabilities like shellshock and heartbleed have also shown that an exploit in one component can also be used to access others thro ugh buffer overflows,
memory overruns etc. and/or impact the immunity of system severely.

Cannot always blame databases here.

BACKUPS?

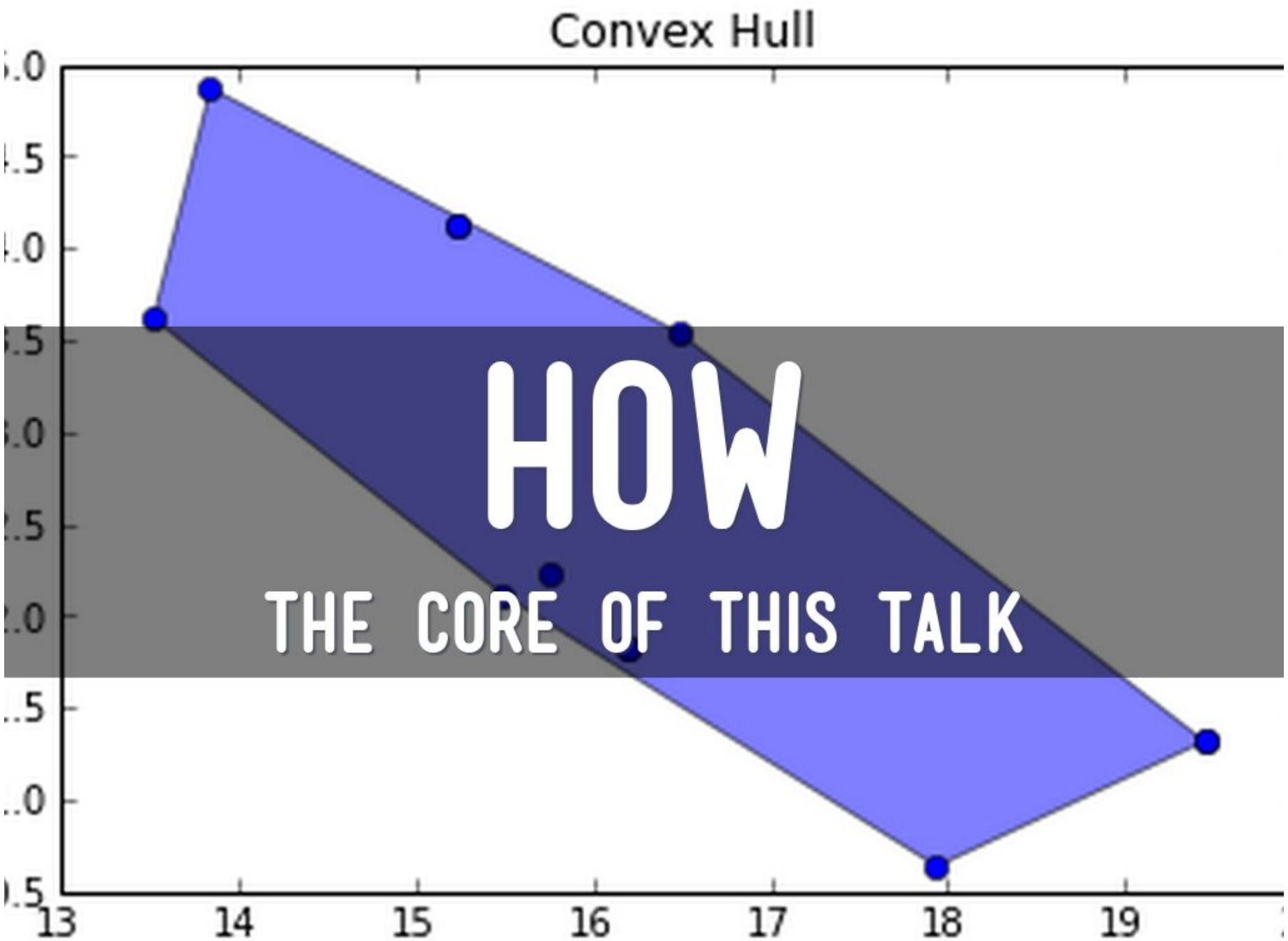
DO THEY HELP? 'MAY BE'

not if they are also corrupted

Maintain logs - journalctl

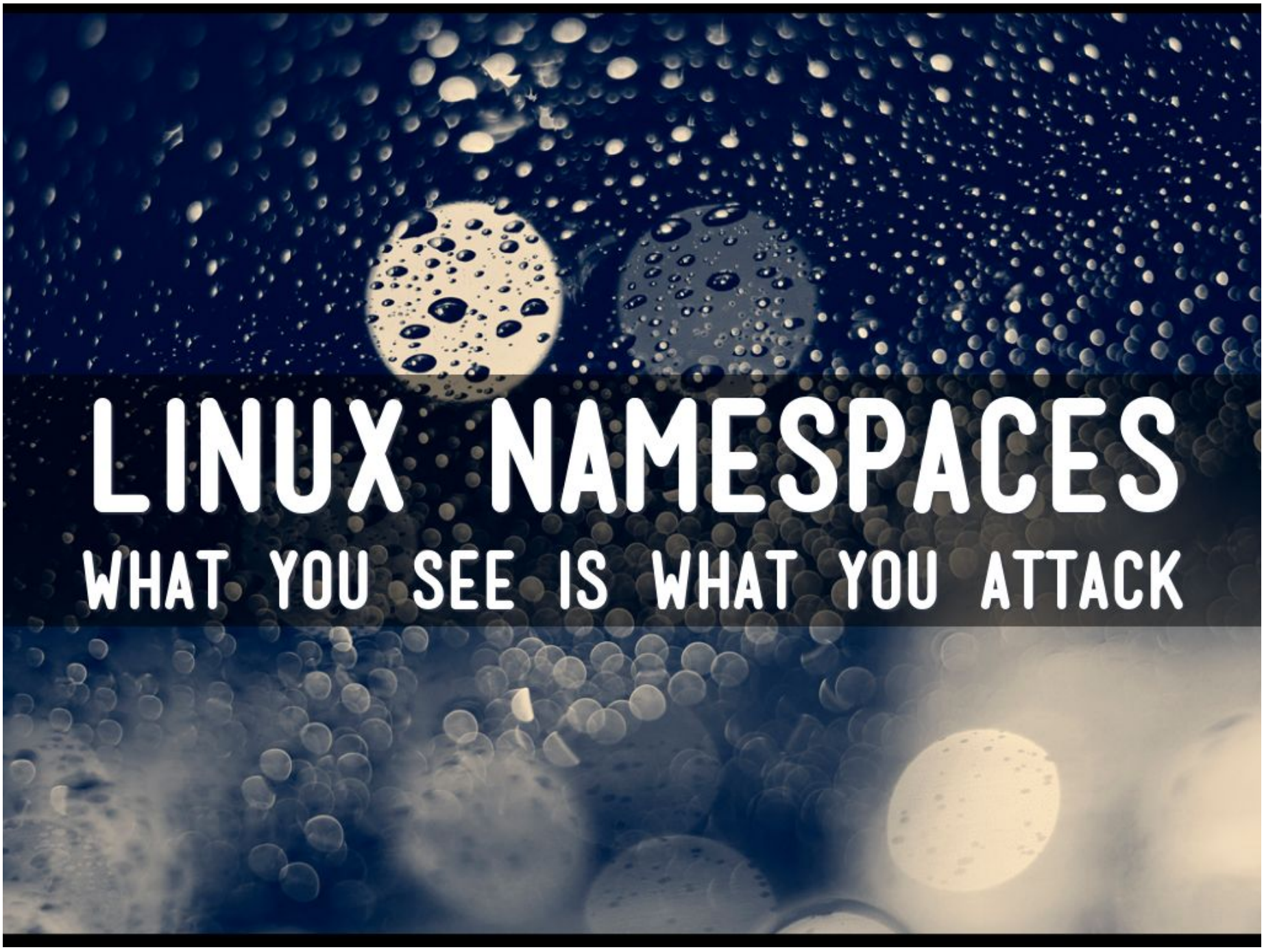
FSS

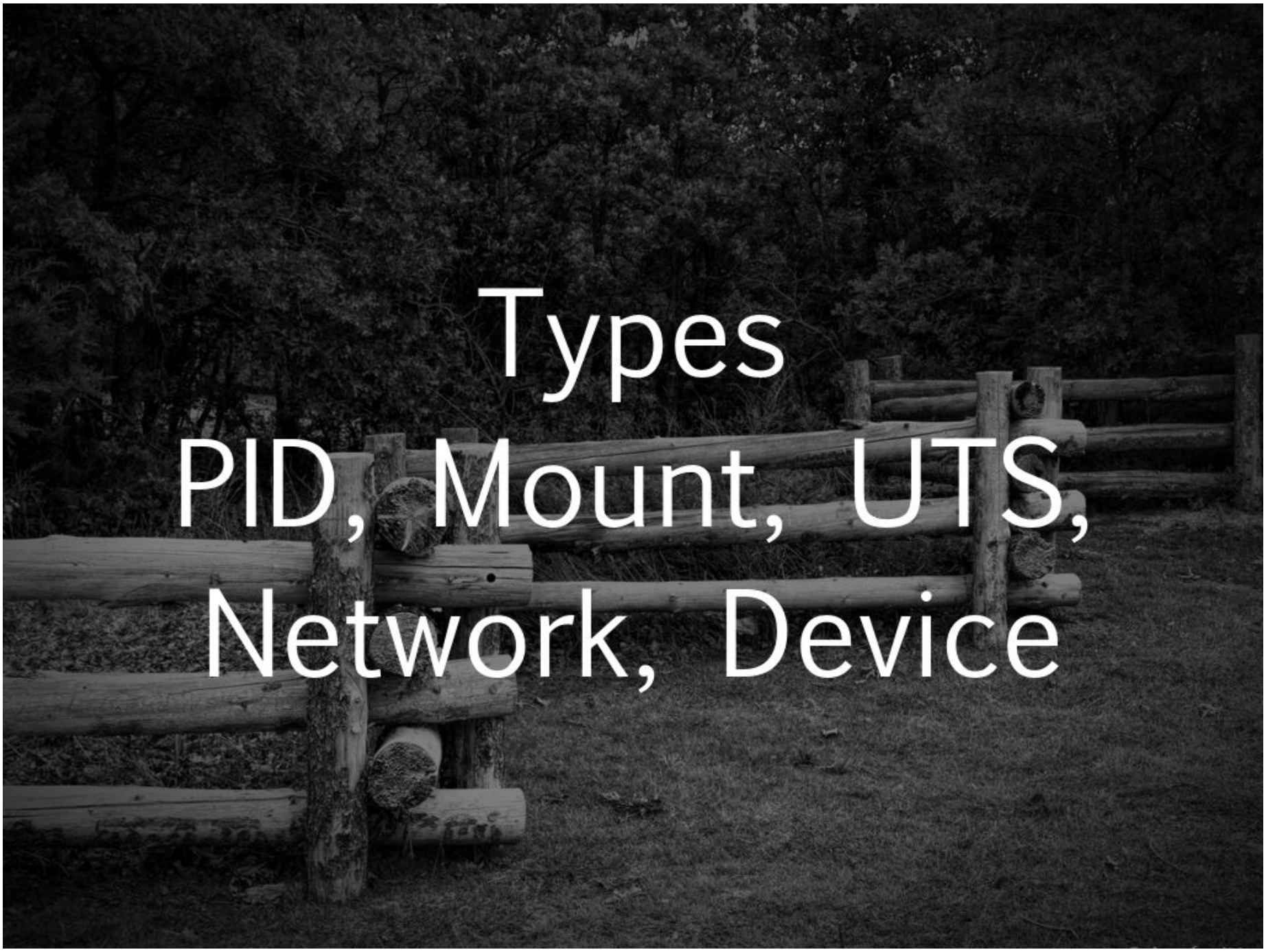
This is where "Principle of least privilege" comes into play. Wikipedia defines it as "a particular abstraction layer of a computing environment, every module (such as a process, a user or a program depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose".

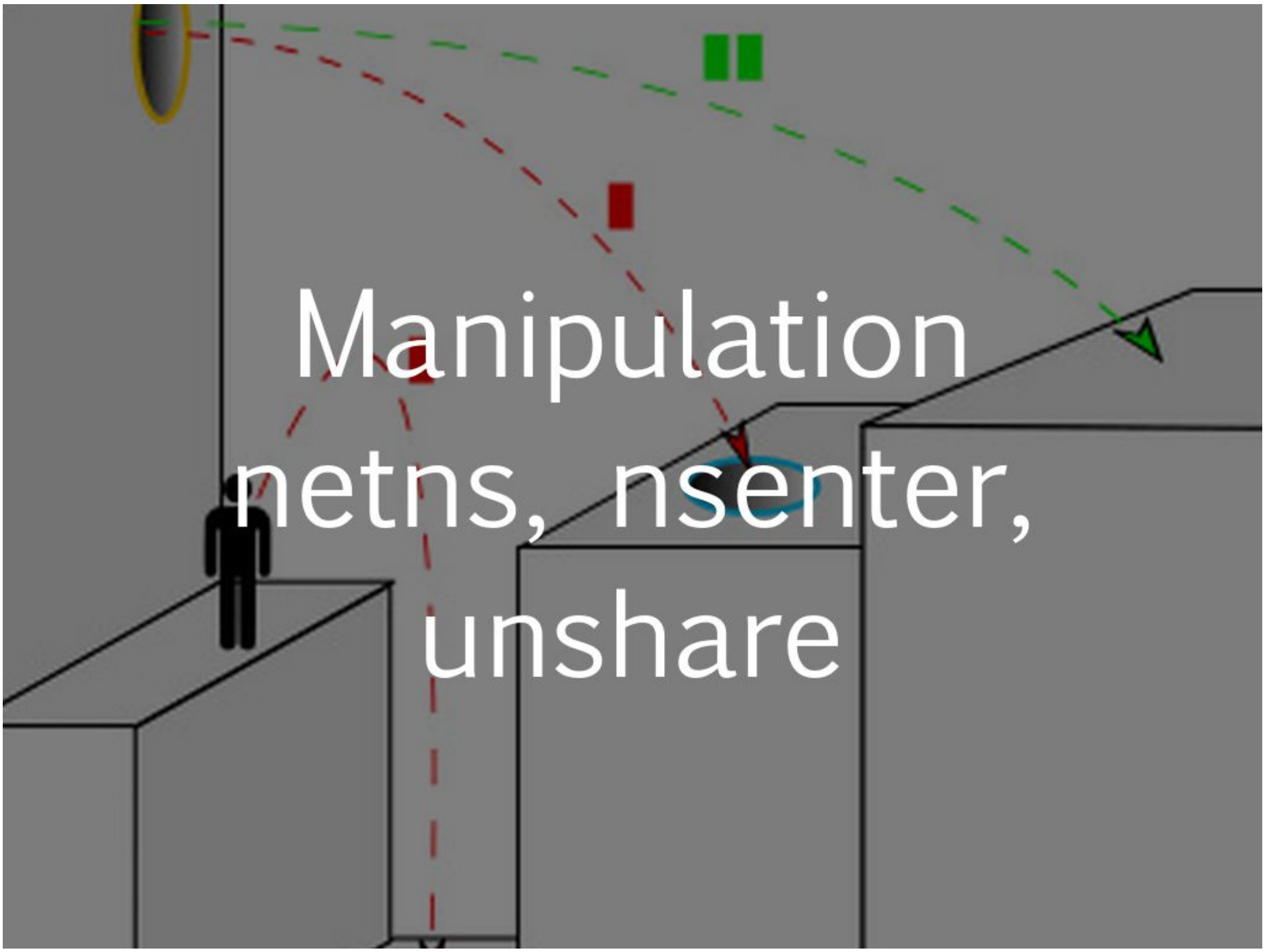


HOW

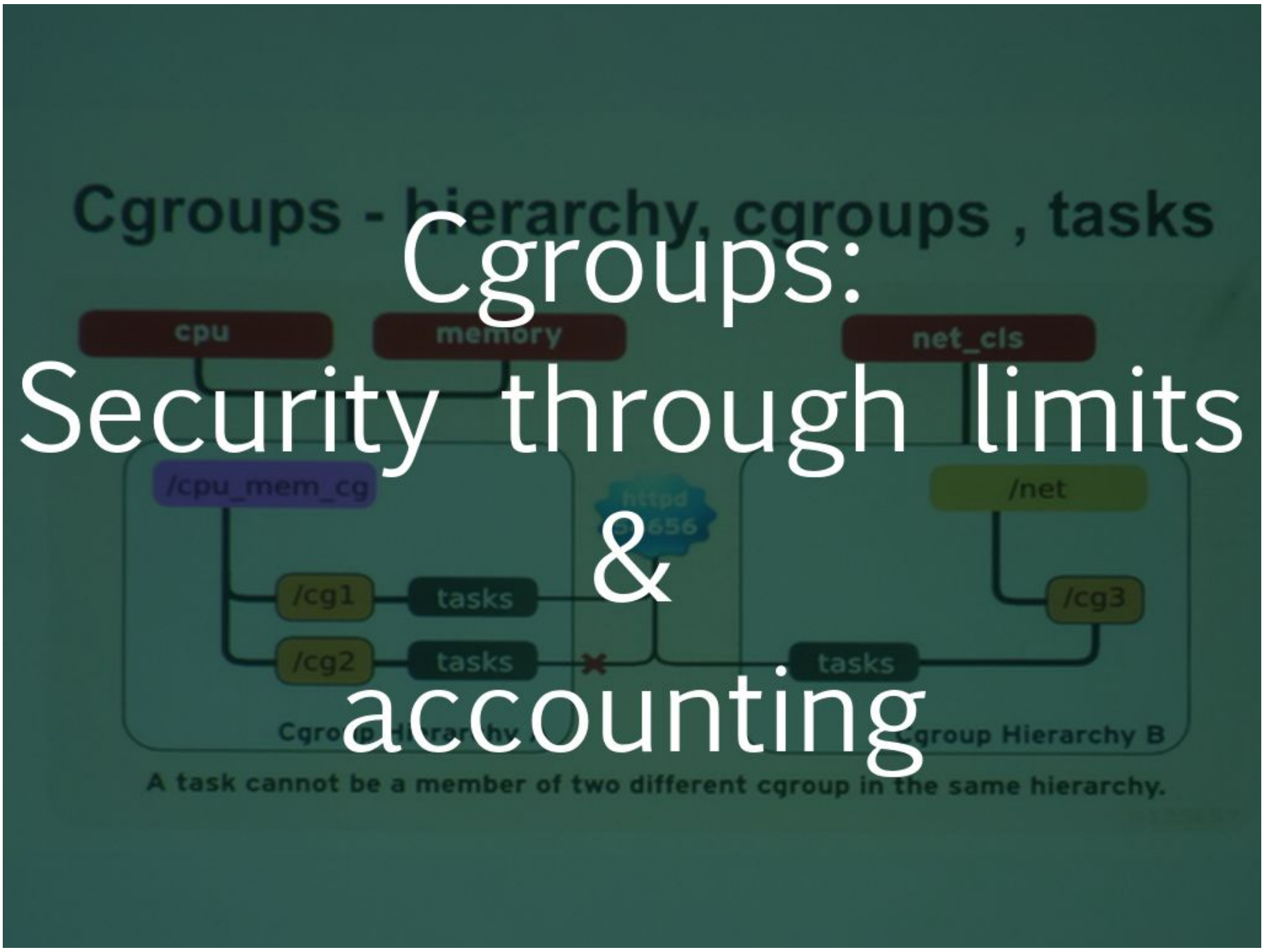
THE CORE OF THIS TALK



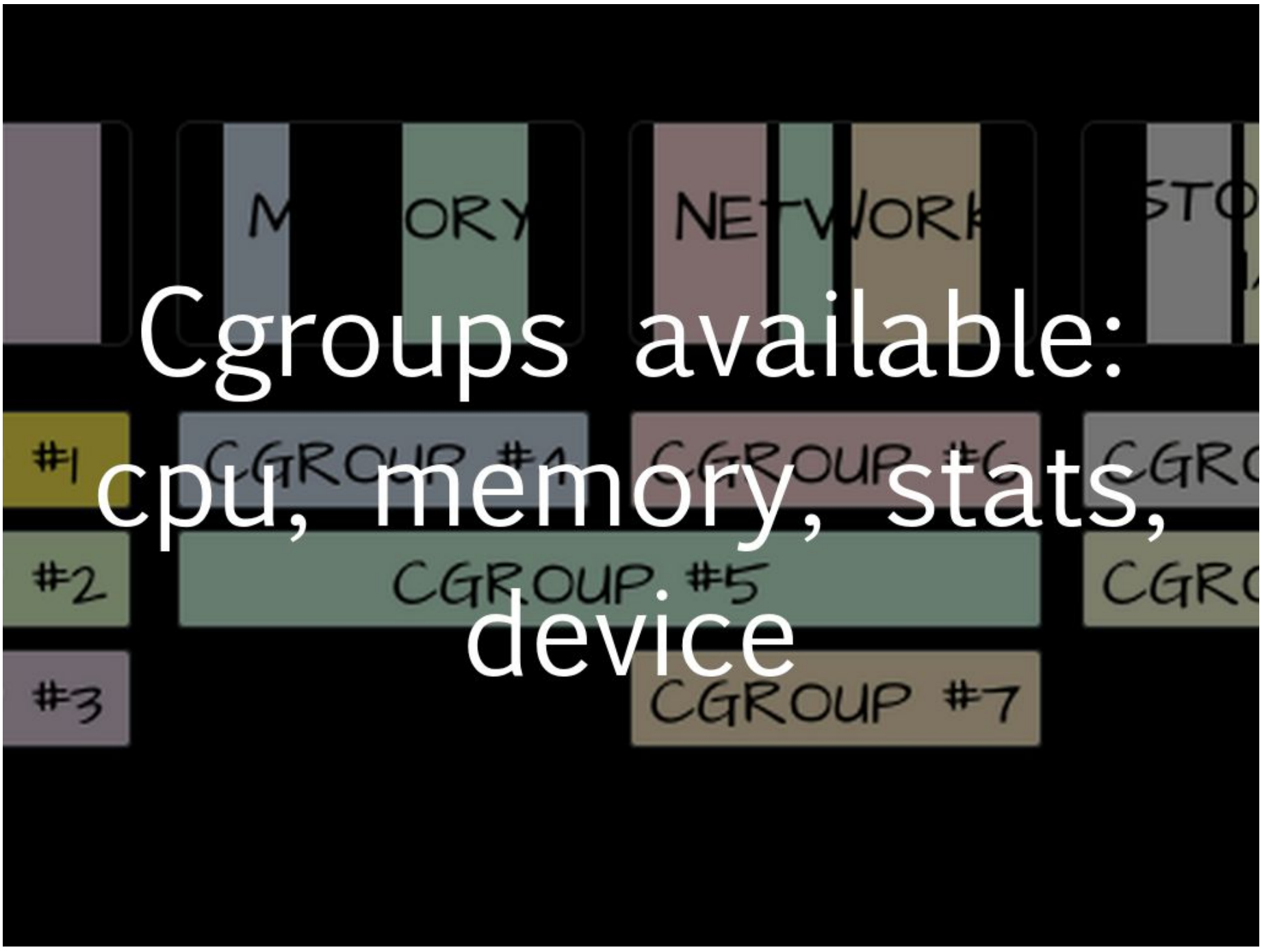


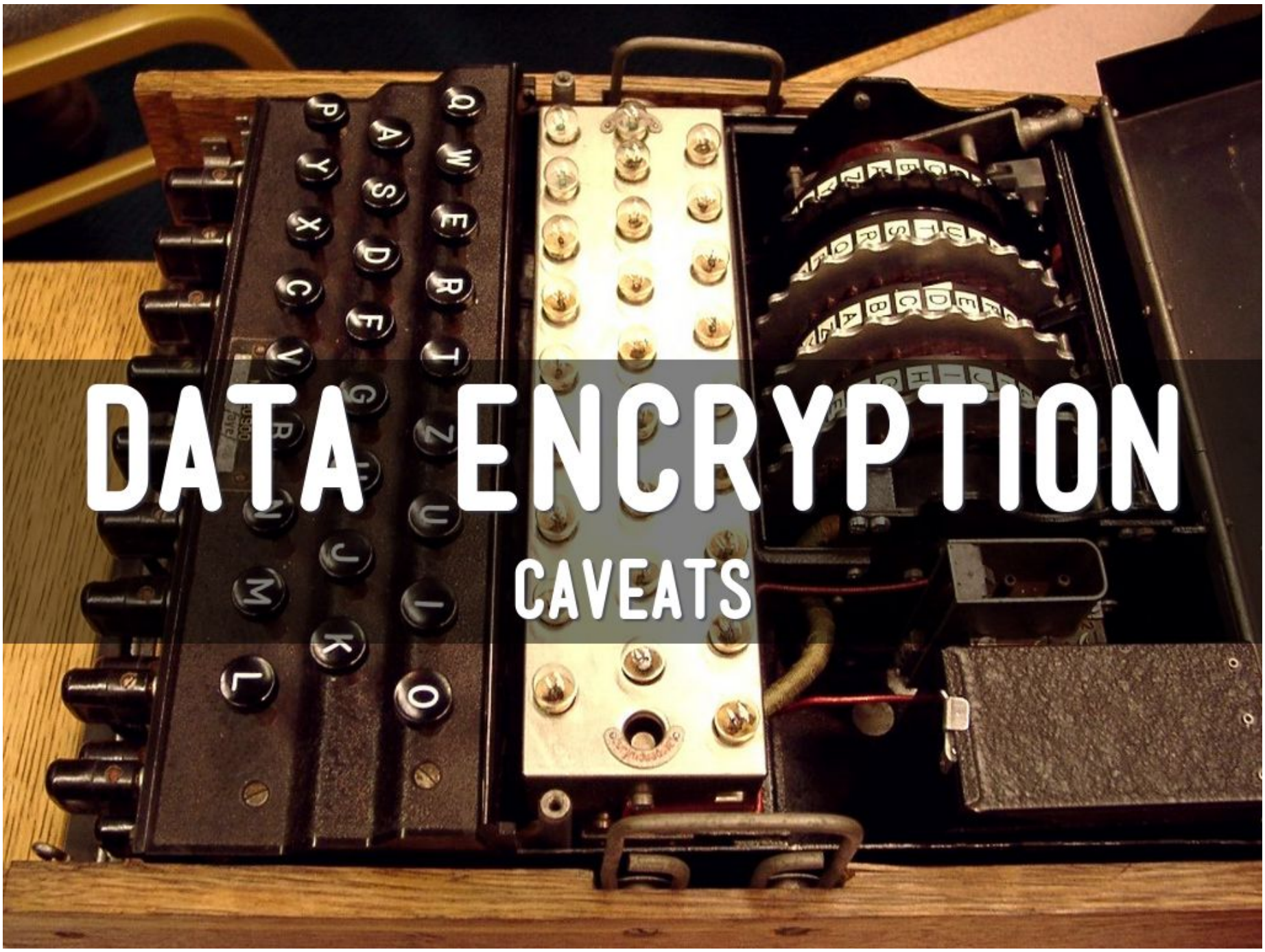


Linux capabilities have been quite underused since their inception in linux. Barring CAP_SYS_ADMIN, all other capabilities allow for fine grained allocation
of privileges to processes. Containers like docker already allow for a container to be run with privileges instead of a fully privileged container



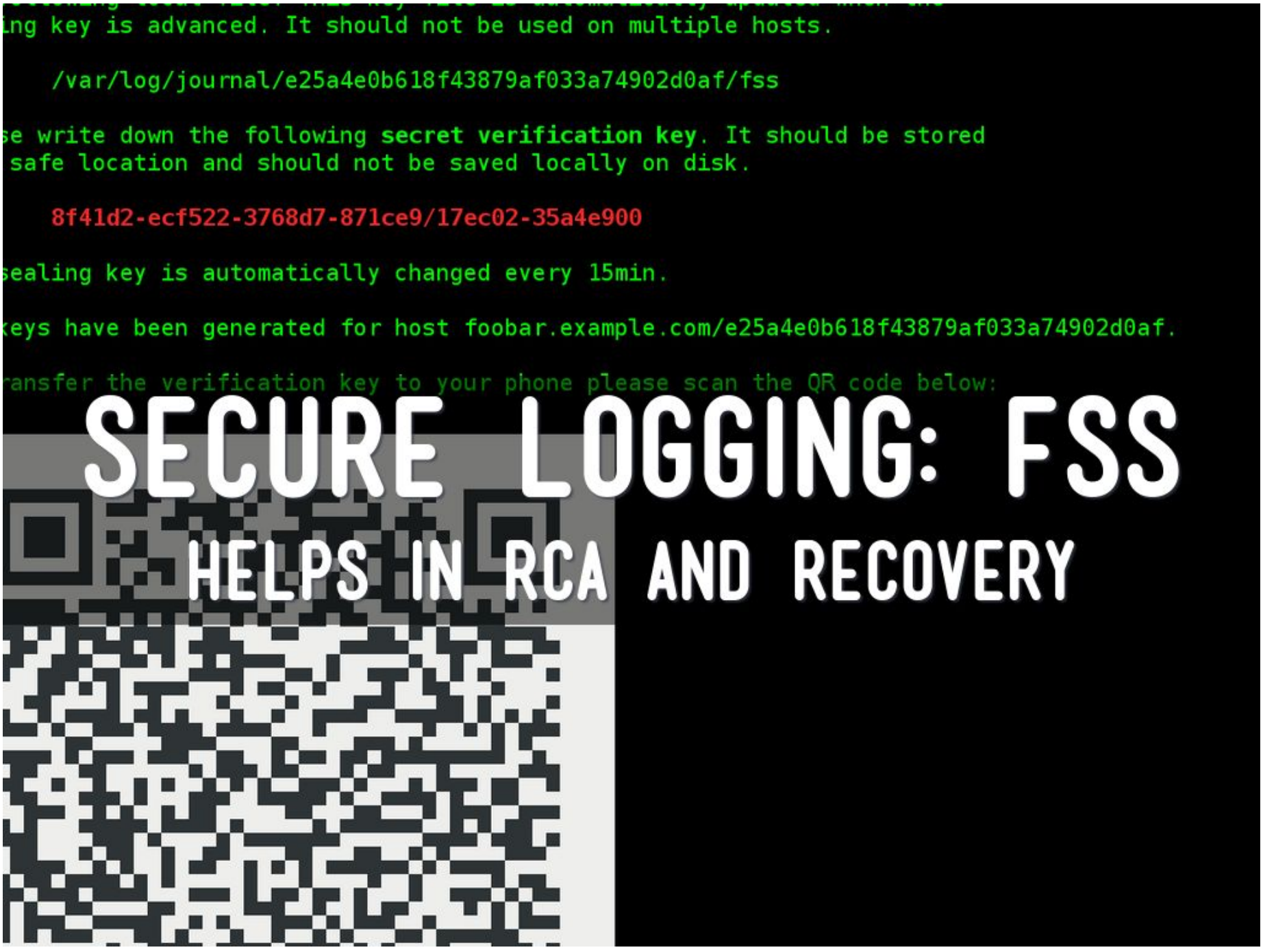
Cgroups: Security through limits & accounting





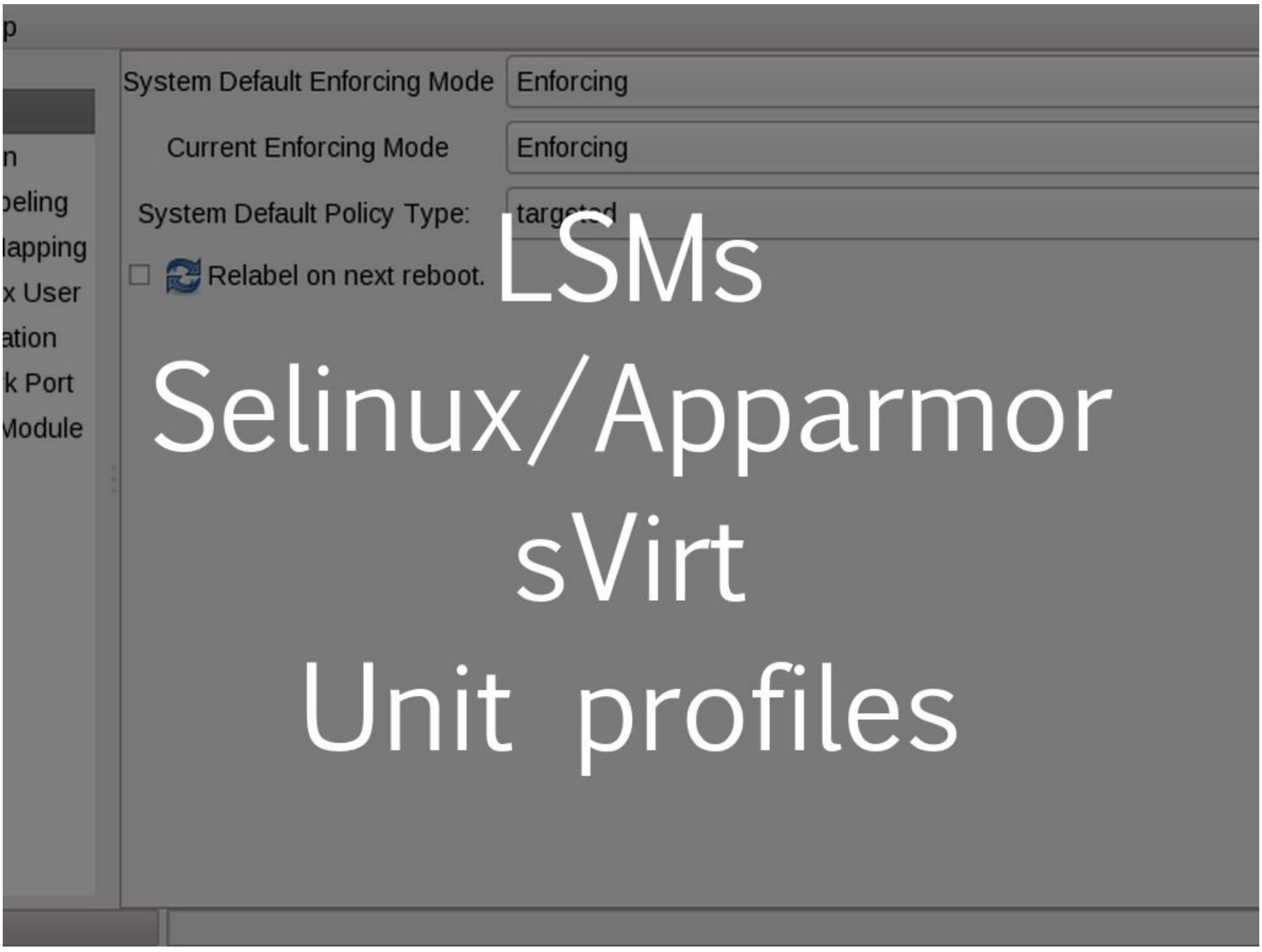
DATA ENCRYPTION

CAVEATS



VIRTUALIZATION?

- Container(s) inside a VM?
- Not far fetched for pods
- Also,
- Zerovm - NaCl sandbox
- boot2docker



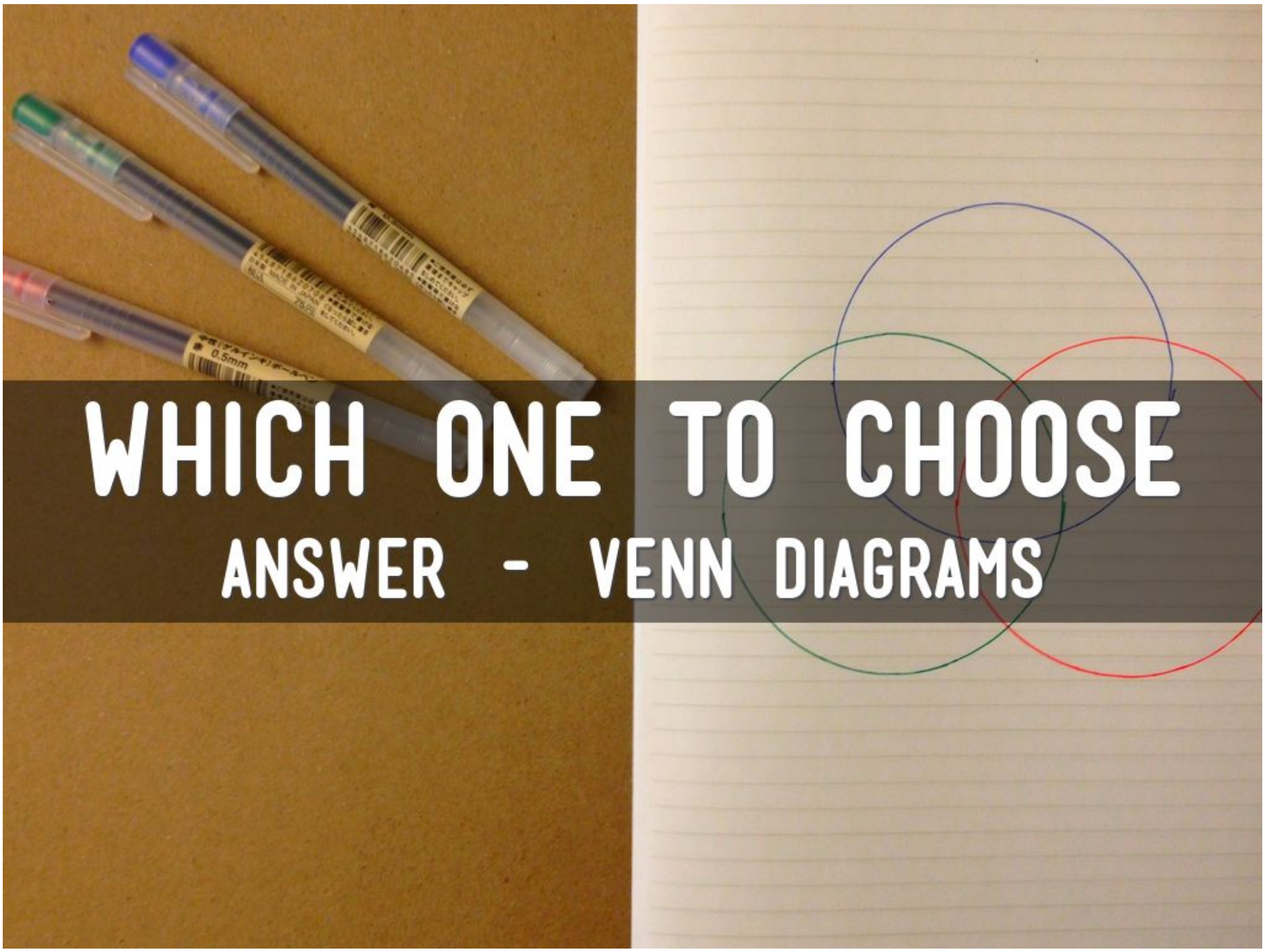
LSMs
Selinux/Apparmor
sVirt
Unit profiles

FIREWALL!

- Iptables
- Some support in docker
- and systemd - service oriented
- Conntrack and netfilter for labels
- traffic control - tc!

OTHERS

- Ulimits
- UID/GID
- ACL
- DBus
- SUID?



EXAMPLES!

SYSTEMD UNIT FOR MYSQLD

```
[Service]
EnvironmentFile=/etc/sysconfig/mysql
User=mysql
ExecStart=/usr/bin/mysqld  --basedir=/usr
PrivateTmp=true
LimitNOFILE=30000
SystemCallFilter=~ioctl
NoNewPrivileges=yes
SELinuxContext=mysqld_t
ProtectHome=true
PrivateDevices=true
CapabilityBoundingSet=-CAP_SYS_PTRACE
ProtectSystem=full
```

CPUShares=512
MemoryLimit=2G
MemorySoftLimit=1.8G
BlockIOReadBandwidth=/dev/sda 1G
ControlGroupAttribute=memory.swappiness 70

Now, with docker:

```
docker  --iptables=true -d --selinux-enable=true
docker run -u mysql --privileged=false -c 512
--security-opt label:type:mysqld_t
--cap-drop=sys_ptrace
-e MYSQL_ROOT_PASSWORD=test
-v /mysql/dir:/var/lib/mysql
-m 1g --name=mysql-server -p 3306:3306
--net=bridge -d mysql:5.6
```

MORE?

MANIFEST.JSON FOR A PXC POD - ANOTHER TALK!

PHOTO CREDITS!

- www.incapsula.com/images/blog/images/2014-mega-vulnerabilities.png
- i1.wp.com/duffy.fedorapeople.org/blog/designs/cgroups/diagram2.png
- noflex.org/wp-content/uploads/2014/09/journald-fss.png
- upload.wikimedia.org/wikipedia/commons/f/f1/Sandbox_with_toys_detail.JPG