Virtual Machine
Impact on Entropy in Guest System

Intern: Ujwal Komarla
Mentor: Dave King
Manager: Manish Gaur
Team: vSECR

Does using Virtual Machines break the keystone of cryptographic services – 'The Entropy'

Computers are deterministic and inherently predictable, posing a risk to privacy.

The best solution was

Possibly, the weakest link too.

And...

Virtualization takes that link down and now, you are 'network'.

Analysis

/dev/urandom

- Quantity
  - >Host vs Guest OS: Ubuntu – 347kB/s vs 337kB/s
  - >Distributions:
    - Ubuntu 336kB/s
    - CentOS 500kB/s
    - Ttylinux 421kB/s
    - ESXi 102kB/s
  - >Workload(Table)

Hypervisor load (Core, Memory, Disk)	Ubuntu	CentOS	ttylinux	ESXi
Single VM (16,10GiB,20GiB)	336kB/s	500kB/s	421kB/s	102kB/s
Parallel VMs reading /dev/urandom (16,10GiB,20GiB)	320kB/s	482kB/s	409kB/s	98kB/s
Parallel VMs reading /dev/urandom (4,2GiB,20GiB)	316kB/s	509kB/s	414kB/s	96kB/s

- Quality
  Identical and acceptable results produced by the de-facto Entropy Test Suite - NIST.
- CSPRNG and seed file keeps the system running even as a VM

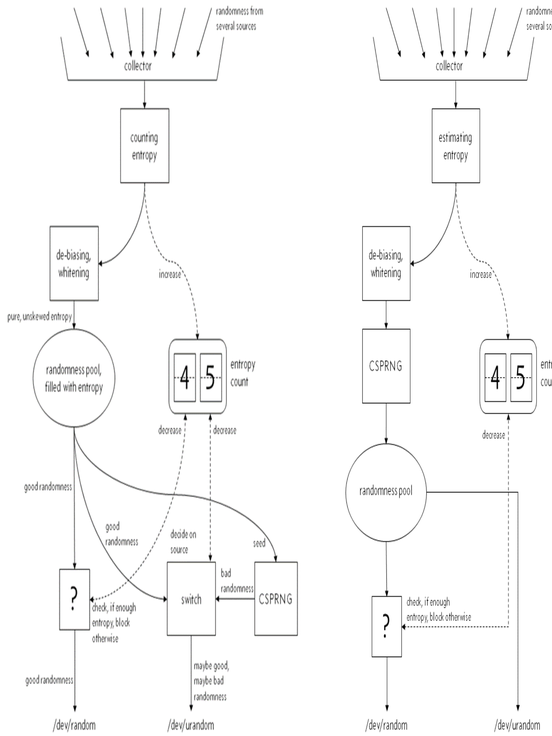
/dev/random

- Quantity
  - > Host vs Guest OS: Ubuntu – 297kB vs 225kB
  - > Reduced Number of Entropy sources : 10 vs 3

Linux Kernel Instrumentation

- To have a view from the system side of the contributors and drainers of entropy
- Tools used : inotifywait, systemtap, d3.js

Myth vs Fact



Reference: 2uo.de/myths-about-urandom/

Future Work

- Correlation and divergence analysis of entropy pool of cloned or forked VM.
- Evaluation of methods to reseed pool when cloning/forking/reverting to a checkpoint of VM

vmware®

NC STATE UNIVERSITY