WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Not-So-Random Numbers

A. Everspaugh, Y. Zhai, R. Jellinek, T. Ristenpart, M. Swift

WISDOM

Research Questions

Are system RNGs secure from catastrophic reset vulnerabilities on virtual machines?

Answer: **NO**

Do virtual environments provide system RNGs with entropy-rich inputs?

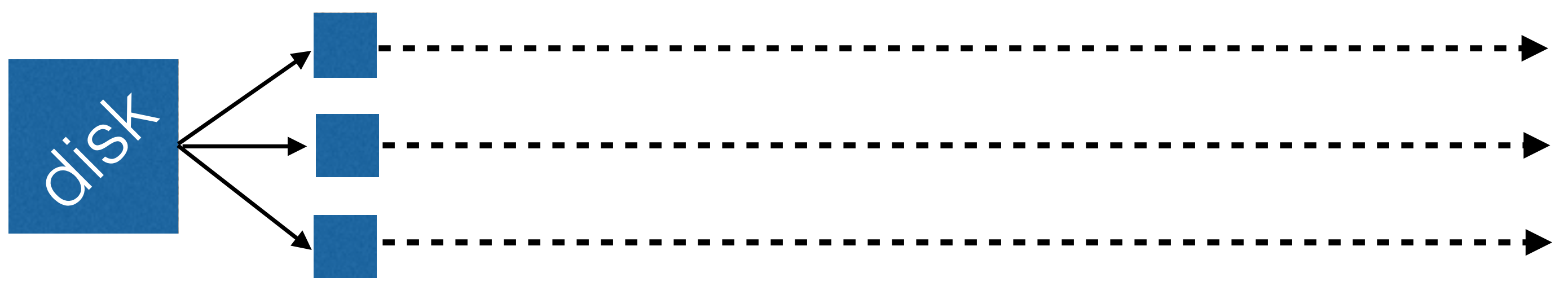
Answer: **YES**

Background

- **Folklore**
  Significant speculation existed on system RNGs in virtual environments [GR05] [SBW09] [RY10], but no measurements had been performed.
- **Reset Security**
  [RY10] showed that reset vulnerabilities exist in Firefox and Apache, but speculated that system RNGs may be more secure.
- **Entropy Estimation**
  Measuring entropy in input sources from an adversary's point of view is critical to determining the security of an RNG. [MWKSS13] provides the only other method known to-date.

Common Cases in Virtual Environments

Boot-from-image



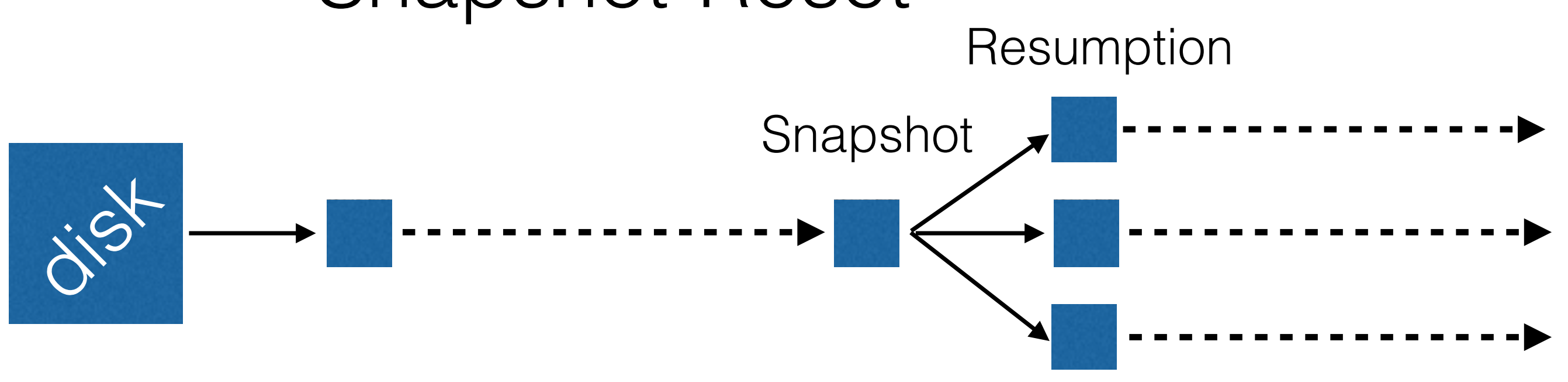
Amazon EC2

Windows Azure

Rackspace

Boot-from-image is the default use case in IaaS clouds. [SBW09] claimed that starting from the same image would lead to predictable outputs — which is not correct.

Snapshot-Reset



vmware

Xen

Parallels

Local VMs support full-memory snapshots which are saved to a file. They can be reused multiple times, but stateful system RNGs may produce repeated output on each resumption.

Reset Vulnerabilities

What is a reset vulnerability?

If a snapshot is used multiple times, a stateful system RNG may produce repeated outputs.

Which systems are vulnerable?

Microsoft Windows 7
`rand_s, CryptGenRandom,`
`RngCryptoServices`

Linux `/dev/(u)random`

FreeBSD `/dev/random`

What's the impact?

Any applications relying on random numbers from system RNGs for security are at risk.

As a proof-of-concept, we've generated identical RSA private keys with OpenSSL after resumption.

Whirlwind RNG

- **Rest Security**
  Whirlwind RNG has reset-security "baked-into" it's design. It uses environmental data during output generation to prevent repeat outputs and has a fast entropy pool that recovers quickly upon reset.
- **Cryptographically Sound**
  The Linux (legacy) RNG is an ad-hoc design. FreeBSD's Yarrow uses a periodically keyed AES generator. Whirlwind uses SHA-512 hash function to guarantee forward and backward secrecy.

References

[GR05] Garfinkel, Rosenblum. When Virtual is Harder than Real. HOTOS 2005.

[RY10] Ristenpart, Yilek. When Good Randomness Goes Bad. NDSS 2010.

[SBW09] Becher, Stamos, Wilcox. Cloud Computing Models and Vulnerabilities. BlackHat 2009.

[MWKSS13] Mowery, Wei, Kohlbrenner, Swanson, Shacham. Welcome to the Entropics. IEEE S+P 2013.