Apple, Google, Microsoft, and others express ‘deep concerns’ over controversial encryption bill

Coalitions representing major tech companies warn of 'unintended consequences' in letter to US senators

By Amar Toor on April 20, 2016 04:37 am Email @amartoo

Four coalitions representing Apple, Microsoft, Google, Amazon, and other major companies have published an open letter expressing their concerns over a controversial US bill that would require smartphone makers to decrypt data on demand. The letter, published this week, is addressed to the bill's sponsors, Sen. Richard Burr (R-NC) and Dianne Feinstein (D-CA), and signed by four industry groups: Reform Government Surveillance, the Computer and Communications Industry Association, the Internet Infrastructure Coalition, and the Entertainment Software Association. In addition to Apple, Microsoft, Google, and Amazon, the coalitions represent companies like Facebook, Netflix, eBay, and Dropbox.

"Any mandatory decryption requirement, such as that included in the discussion draft of the bill that you authored, will to lead to unintended consequences," the letter reads. "The effect of such a requirement will force companies to prioritize government access over other considerations, including digital security." The groups go on to note that adhering to the bill's requirements would make any products or services vulnerable to exploitation by "bad actors," and that it could have major ripple effects. "[N]o accessibility requirement can be limited to U.S. law enforcement," the letter continues, "once it is required by the U.S., other governments will surely follow."

virtualization & cloud computing

cs642

computer security

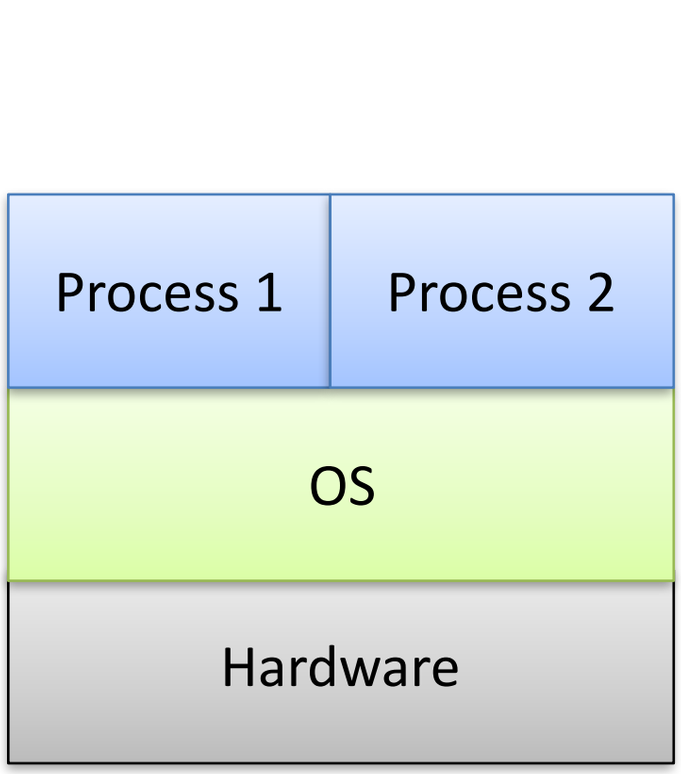
adam everspaugh

ace@cs.wisc.edu

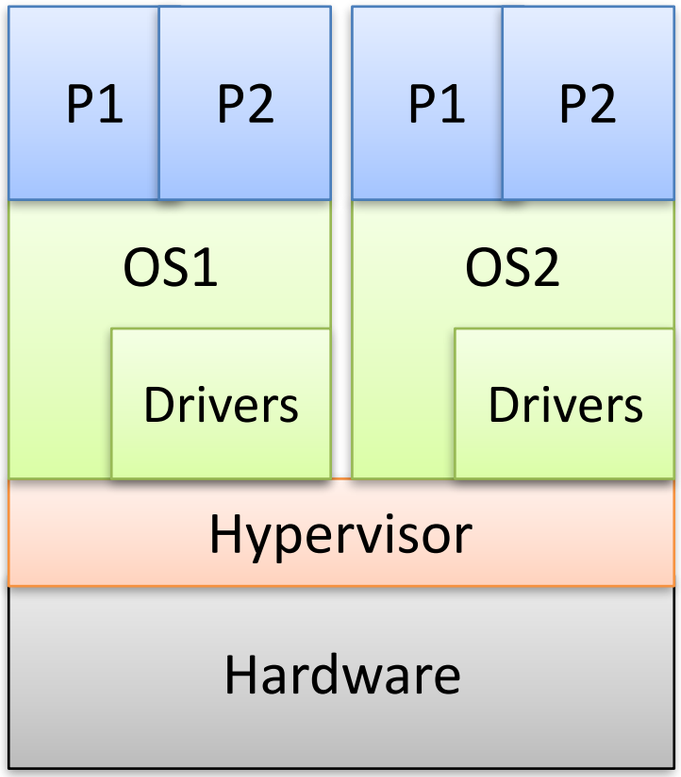
today

* **Announcements:** HW4 posted yesterday
* Virtualization
* Random number generators and reset vulnerabilities
* Cloud computing and co-residency

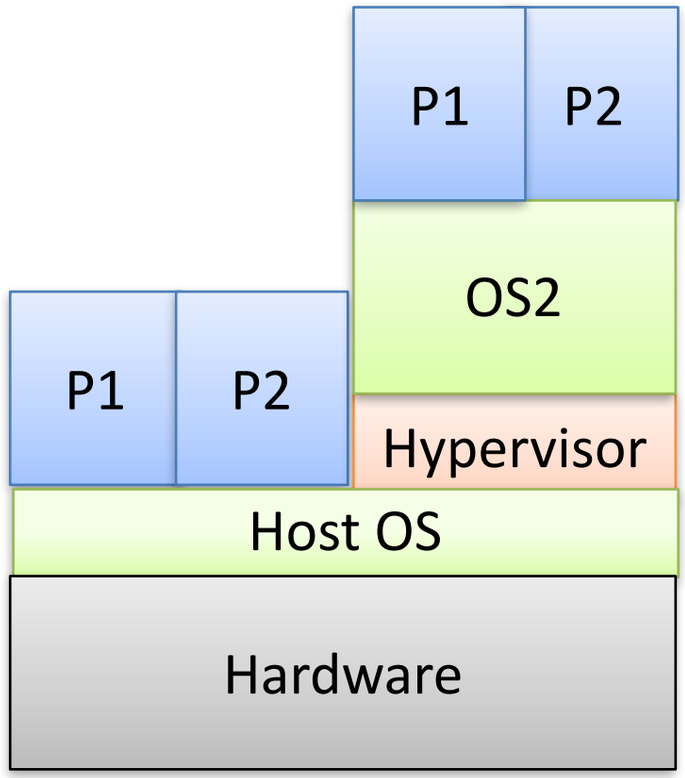
Virtualization



No virtualization



Type-1 Virtualization
(Xen, VMware ESX)



Type-2 Virtualization
(VMware Workstation,
Virtual Box)

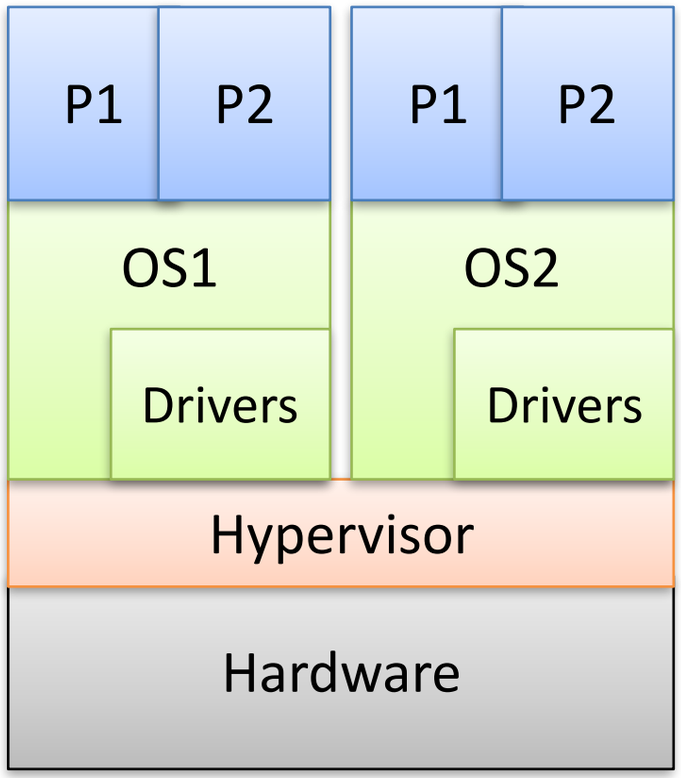
Type-1: Hypervisor runs directly on hardware

Type-2: Hypervisor runs on host OS

VM Use Cases

- Development and testing (especially when we need different OSs)
- Server consolidation
  - Run multiple servers on same hardware: web server, file server, email servers, …
- Cloud computing: Infrastructure-as-a-Service
- Sandboxing / containment

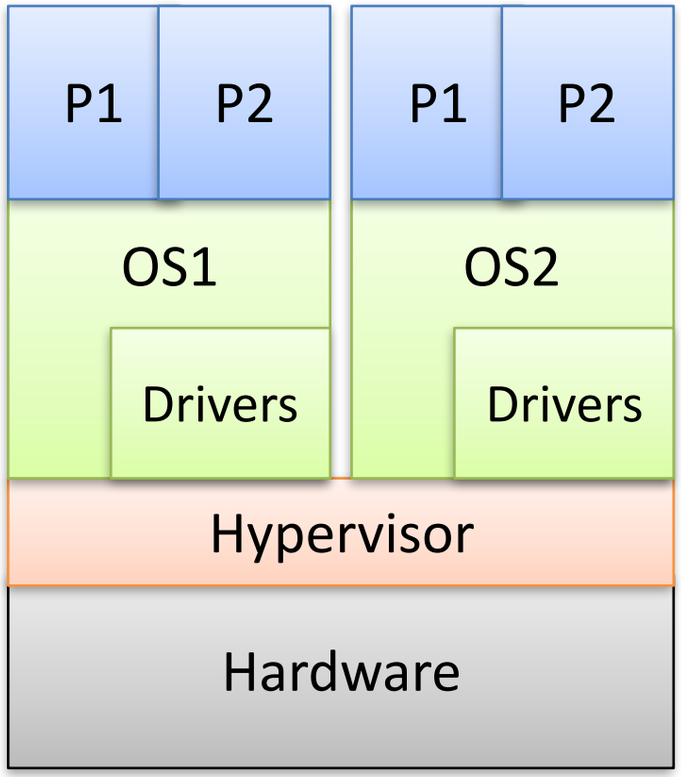
Security Model



Type-1 Virtualization (VMware Workstation, Virtual Box)

- What's the desired security model?
- Isolation between OS1/OS2 (and processes)
  - No access to file system, memory pages
- No "escape" from process/OS to hypervisor
- What can go wrong?

Isolation Problems



Type-1 Virtualization (VMware Workstation, Virtual Box)

- Information leakage
  - side-channel attacks using shared resources (instruction/memory caches)
- Degradation of service
  - Violate performance isolation, OS1 degrades OS2 to get more CPU time or network bandwidth
- Other problems?

Virtual Machine Management

- Snapshots
  - Volume snapshot / checkpoint
    - persistent storage of VM
    - must boot from storage when resuming snapshot
  - Full snapshot
    - persistent storage and ephemeral storage (memory, register states, caches, etc.)
    - start/resume in between (essentially) arbitrary instructions
- VM image is a file that stores a snapshot

Uses for Secure Random Numbers

Cryptography

- Keys
- Nonces, initial values (IVs), salts

System Security

- TCP Initial Sequence Numbers (ISNs)
- ASLR
- Stack Canaries

Where can we get secure random numbers?

Every OS provides a high-quality RNG

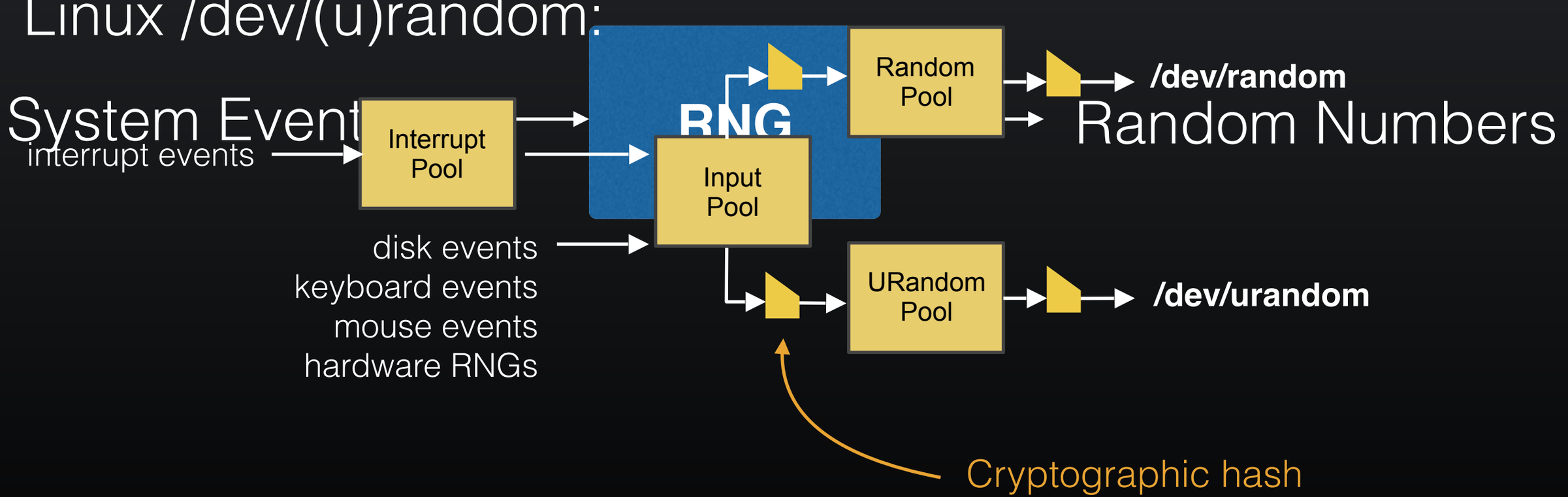
OSX/Linux:

```
cat /dev/urandom
```

Operating System Random Number Generators

Linux RNG

Linux /dev/(u)random:

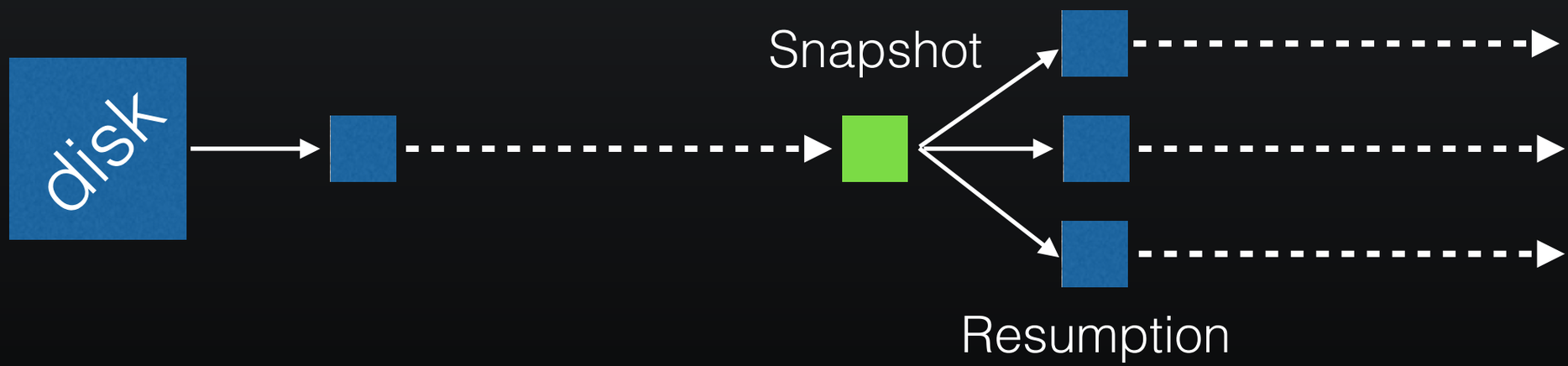


RNG Failures

RNG Failures
Predictable Output
Repeated Output
Outputs from a small range (not-statistically uniform)

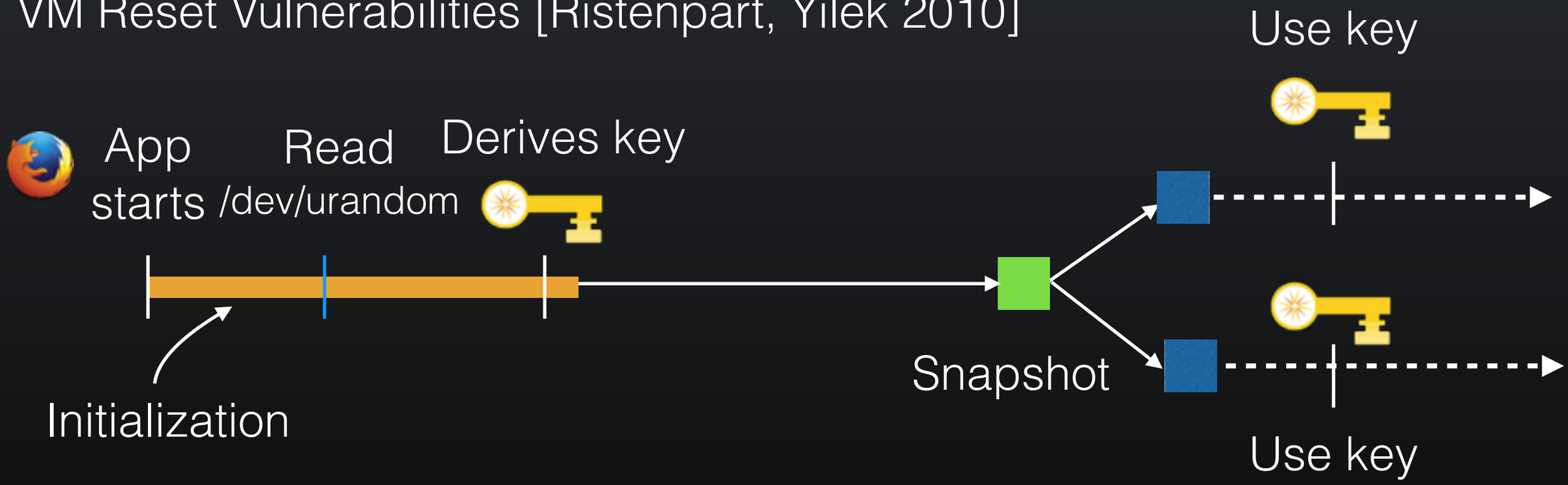
Broken Windows RNG: [DGP 2007]
Broken Linux RNG: [GPR 2008], [LRSV 2012], [DPRVW 2013], [EZJSR 2014]
Factorable RSA Keys: [HDWH 2012]
Taiwan National IDs: [BCCHLS 2013]

Virtual Machine Snapshots



Security Problems with VM Resets

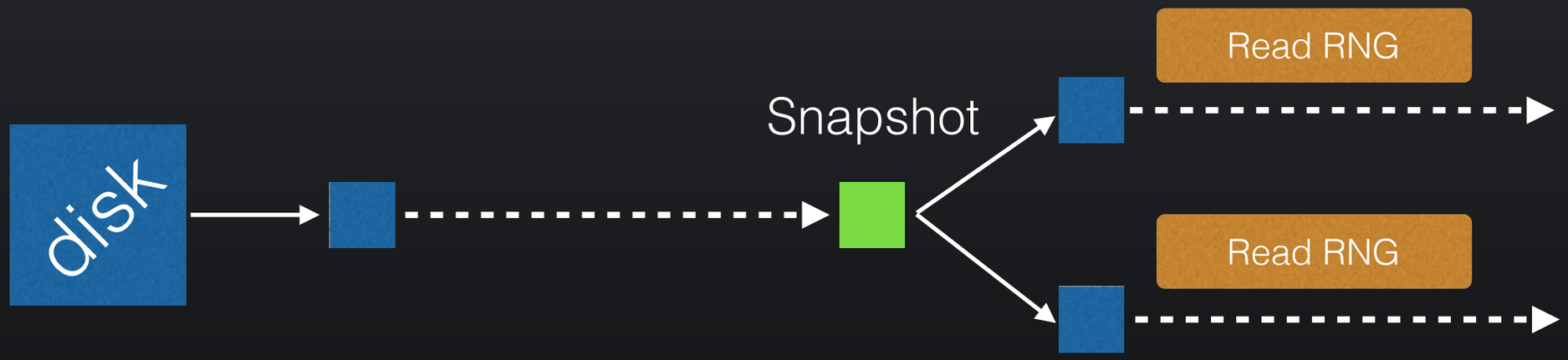
VM Reset Vulnerabilities [Ristenpart, Yilek 2010]



Firefox and Apache reused random values for TLS
Attacker can read previous TLS sessions, recover private keys from Apache

Linux RNG after VM Reset

Not-So-Random Numbers in Virtualized Linux
[Everspaugh, et al, 2014]



Experiment:

- Boot VM in Xen or VMware
- Capture snapshot
- Resume from snapshot, read from /dev/urandom

Repeat: 8 distinct snapshots
20 resumptions/snapshot

/dev/urandom outputs after resumption

Linux RNG is ***not*** reset secure:
7/8 snapshots produce mostly identical outputs

Reset 1	Reset 2	Reset 3
1E6DD331	1E6DD331	1E6DD331
8CC97112	8CC97112	8CC97112
2A2FA7DB	2A2FA7DB	2A2FA7DB
DBBF058C	DBBF058C	DBBF058C
26C334E7	26C334E7	26C334E7
F17D2D20	F17D2D20	45C78AE0
CC10232E	CC10232E	E678DBB2
...	...	...

Reset insecurity and applications

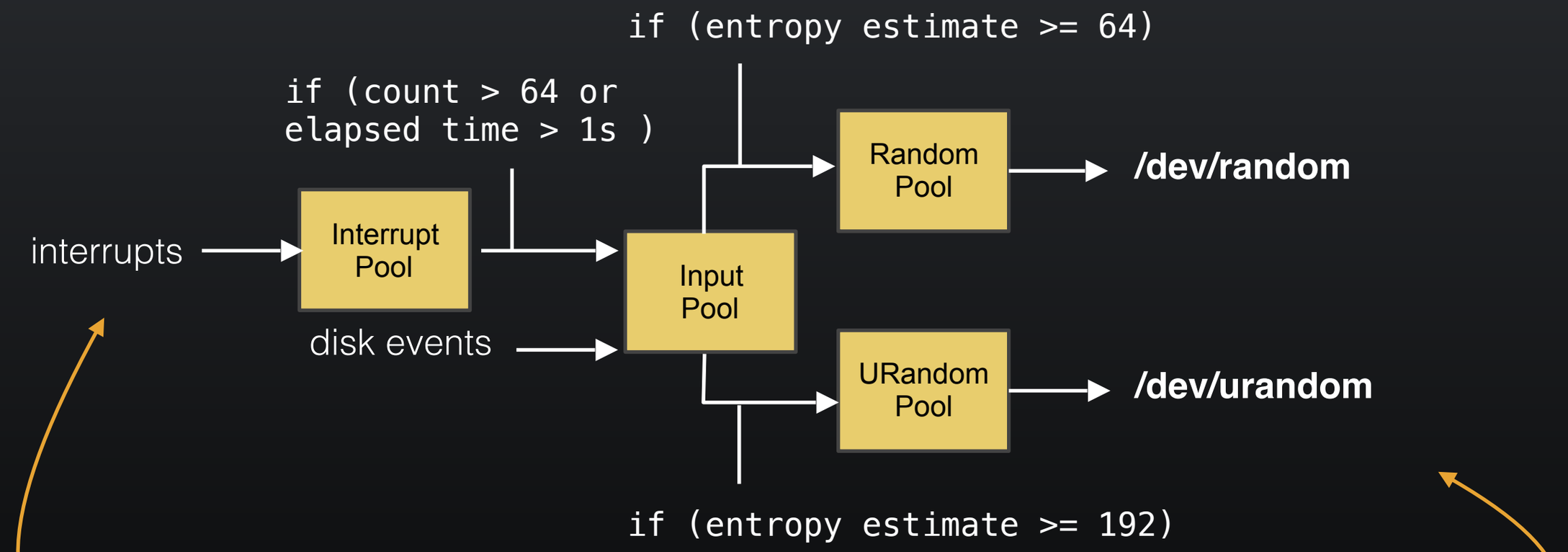
Generate RSA key on resumption:

```
openssl genrsa
```

30 snapshots; 2 resets/snapshot (ASLR Off)

- 27 trials produced identical private keys
- 3 trials produced unique private keys

Why does this happen?



Buffering and thresholds prevent new inputs from impacting outputs

Linux /dev/(u)random

What about other platforms?

FreeBSD

/dev/random produces identical output stream
Up to 100 seconds after resumption

Microsoft Windows 7

Produces repeated outputs indefinitely

`rand_s`	(stdlib)
`CryptGenRandom`	(Win32)
`RngCryptoServices`	(.NET)

INTERMISSION

Cloud computing

Cloud providers

Popular customers

Who can be a customer?

We call these "public clouds"

VMs
Infrastructure-as-a-service

Storage

Web Cache/TLS Termination

AWS | Services | Edit

Amazon Web Services

Compute

EC2
Virtual Servers in the Cloud

EC2 Container Service
Run and Manage Docker Containers

Elastic Beanstalk
Run and Manage Web Apps

Lambda
Run Code in Response to Events

Storage & Content Delivery

S3
Scalable Storage in the Cloud

CloudFront
Global Content Delivery Network

Elastic File System PREVIEW
Fully Managed File System for EC2

Glacier
Archive Storage in the Cloud

Snowball
Large Scale Data Transport

Storage Gateway
Hybrid Storage Integration

Database

RDS
Managed Relational Database Service

DynamoDB
Managed NoSQL Database

ElastiCache
In-Memory Cache

Redshift
Fast, Simple, Cost-Effective Data Warehousing

DMS
Managed Database Migration Service

Networking

VPC
Isolated Cloud Resources

Direct Connect
Dedicated Network Connection to AWS

Developer Tools

CodeCommit
Store Code in Private Git Repositories

CodeDeploy
Automate Code Deployments

CodePipeline
Release Software using Continuous Delivery

Management Tools

CloudWatch
Monitor Resources and Applications

CloudFormation
Create and Manage Resources with Templates

CloudTrail
Track User Activity and API Usage

Config
Track Resource Inventory and Changes

OpsWorks
Automate Operations with Chef

Service Catalog
Create and Use Standardized Products

Trusted Advisor
Optimize Performance and Security

Security & Identity

Identity & Access Management
Manage User Access and Encryption Keys

Directory Service
Host and Manage Active Directory

Inspector
Analyze Application Security

WAF
Filter Malicious Web Traffic

Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates

Analytics

EMR
Managed Hadoop Framework

Data Pipeline
Orchestration for Data-Driven Workflows

Internet of Things

AWS IoT
Connect Devices to the Cloud

Game Development

GameLift
Deploy and Scale Session-based Multiplayer Games

Mobile Services

Mobile Hub
Build, Test, and Monitor Mobile Apps

Cognito
User Identity and App Data Synchronization

Device Farm
Test Android, iOS, and Web Apps on Real Devices in the Cloud

Mobile Analytics
Collect, View and Export App Analytics

SNS
Push Notification Service

Application Services

API Gateway
Build, Deploy and Manage APIs

AppStream
Low Latency Application Streaming

CloudSearch
Managed Search Service

Elastic Transcoder
Easy-to-Use Scalable Media Transcoding

SES
Email Sending and Receiving Service

SQS
Message Queue Service

SWF
Workflow Service for Coordinating Application Components

Enterprise Applications

WorkSpaces
Desktops in the Cloud

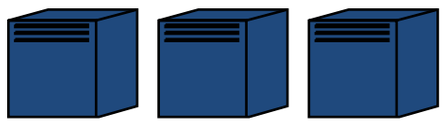
Cloud Services

A simplified model of public cloud computing

Users run Virtual Machines (VMs) on cloud provider's infrastructure

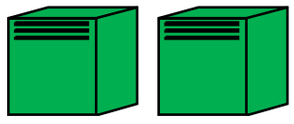
User A

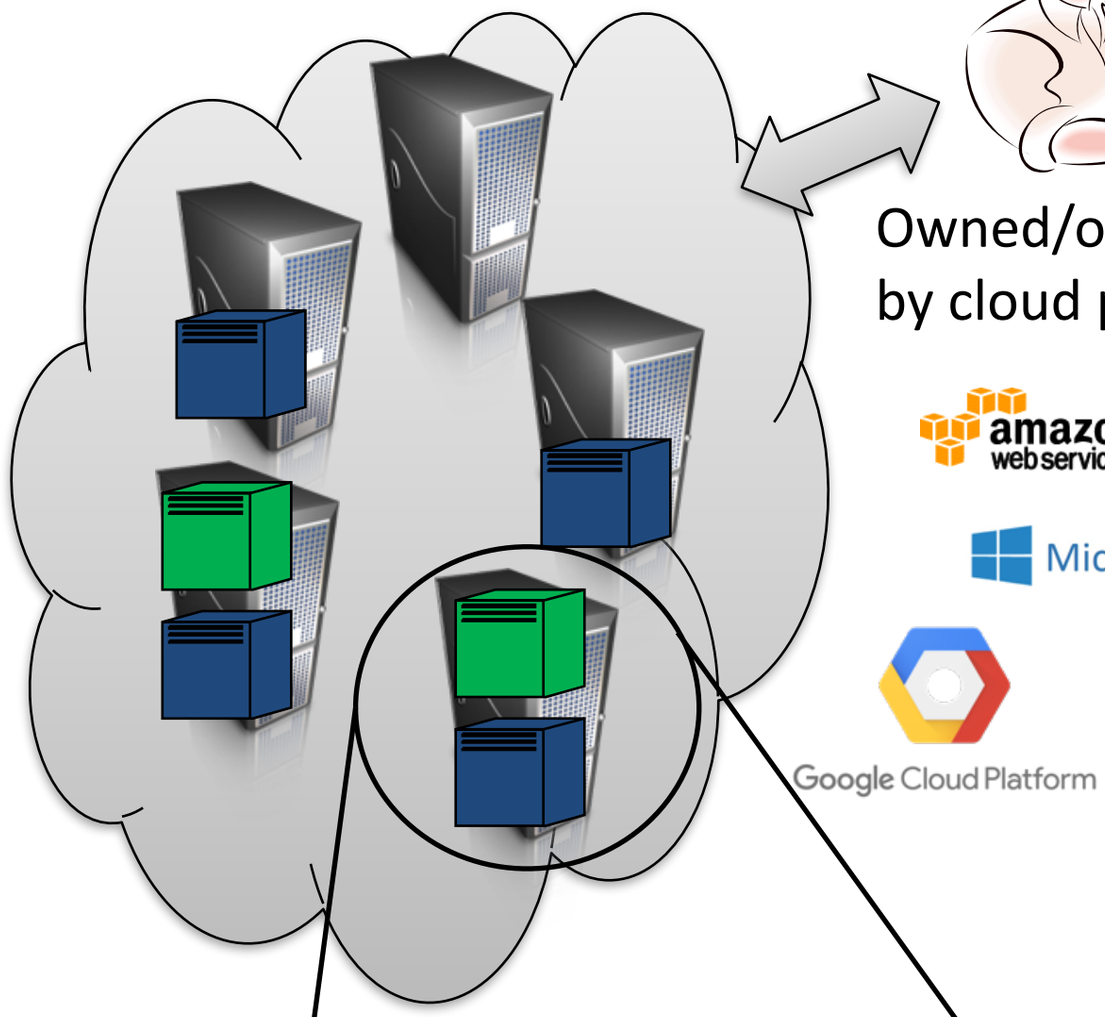
virtual machines (VMs)



User B

virtual machines (VMs)





Owned/operated by cloud provider

amazon web services™

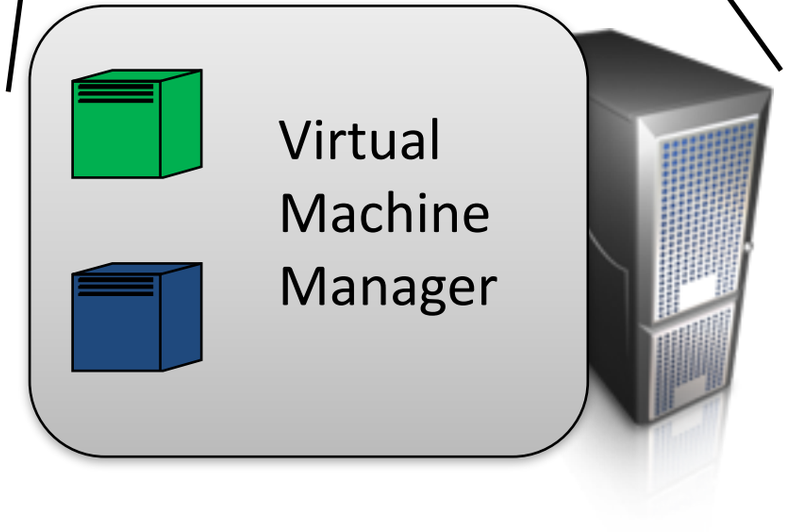
Microsoft Azure

Google Cloud Platform

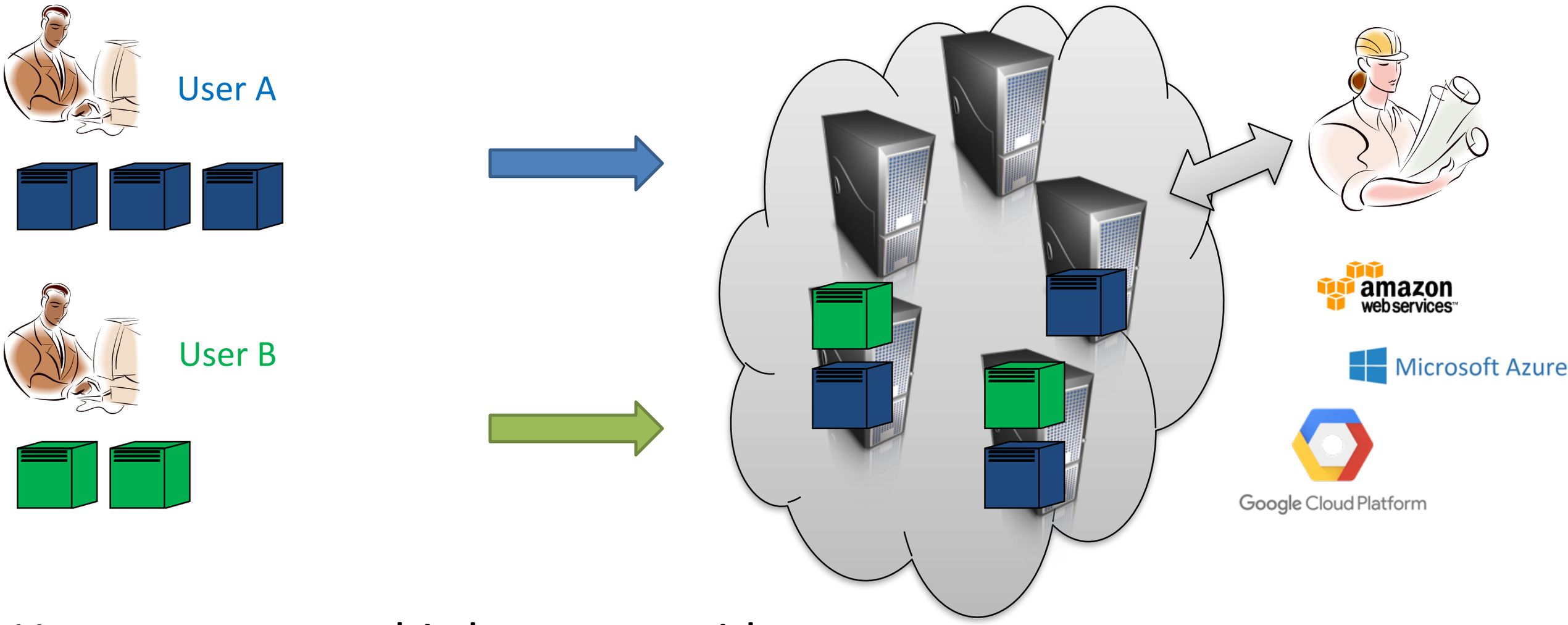
Multitenancy (users share physical resources)

Virtual Machine Manager (VMM) manages physical server resources for VMs

To the VM should look like dedicated server



Trust models in public cloud computing



Users must trust third-party provider to

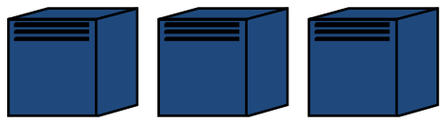
not spy on running VMs / data

secure infrastructure from external attackers

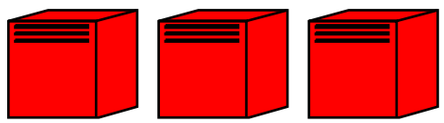
secure infrastructure from internal attackers

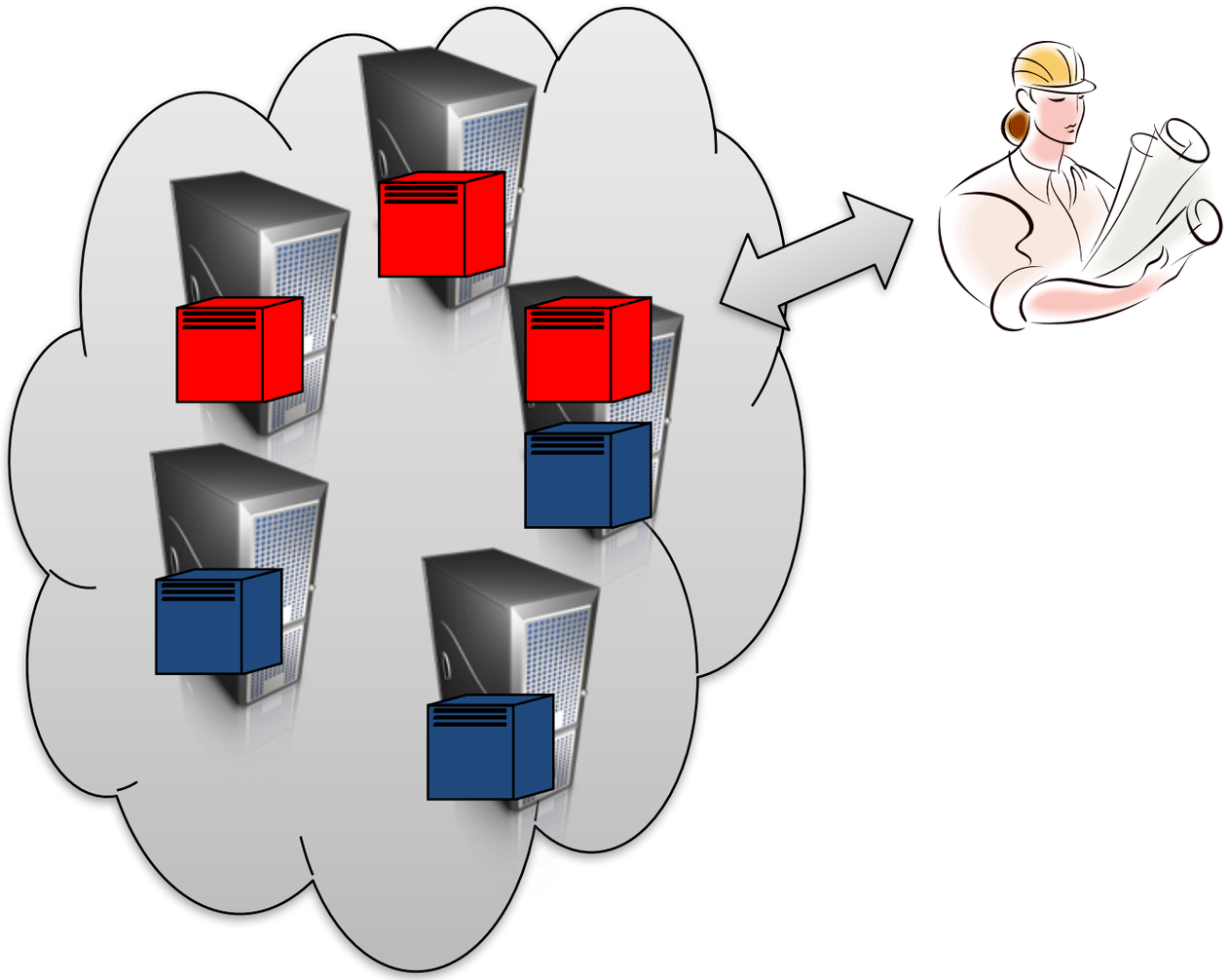
A new threat model:

User A



Bad guy





Attacker identifies one or more victims VMs in cloud

1) Achieve advantageous placement via launching of VM instances

2) Launch attacks using physical proximity

Exploit VMM vulnerability DoS Side-channel attack

Anatomy of attack

Checking for co-residence

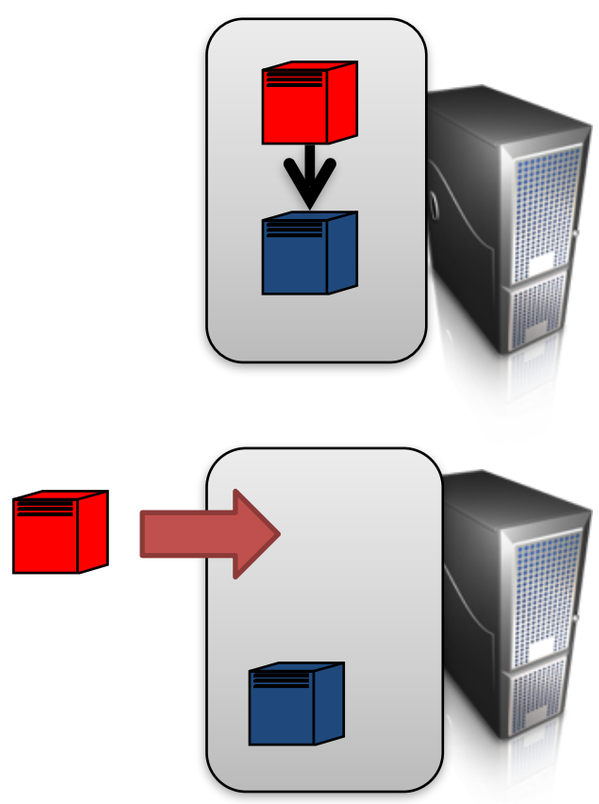
check that VM is on same server as target
- network-based co-residence checks
- efficacy confirmed by covert channels

Achieving co-residence

brute forcing placement
instance flooding after target launches

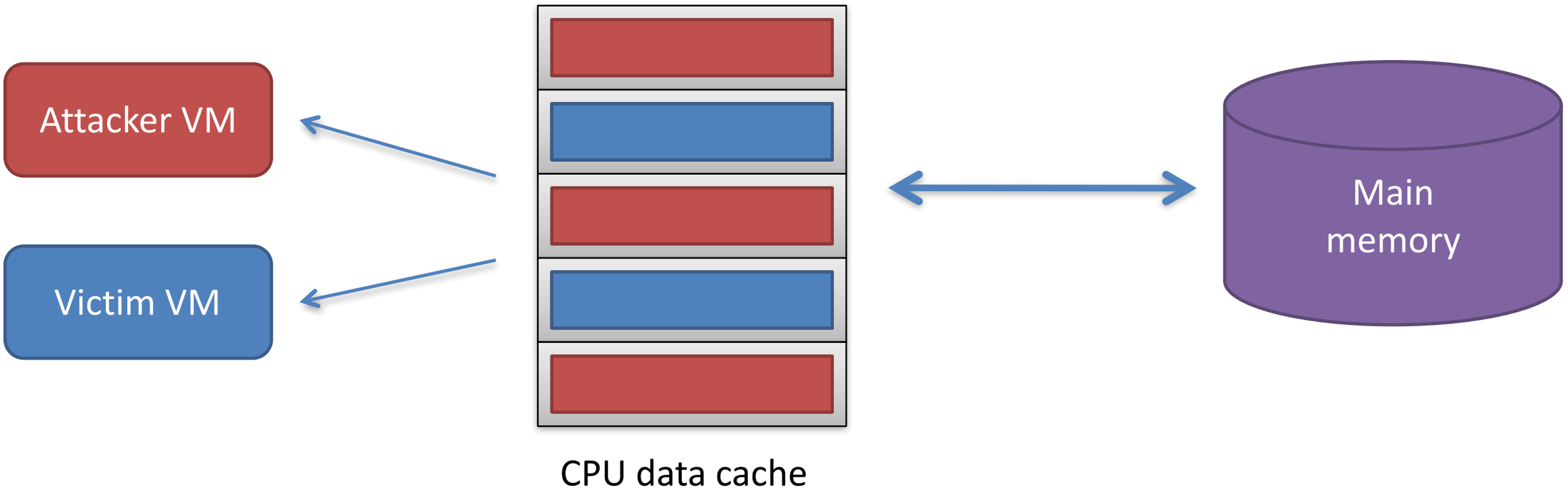
Location-based attacks

side-channels, DoS, escape-from-VM



Placement vulnerability: attackers can knowingly achieve co-residence with target

Cross-VM side channels using CPU cache contention

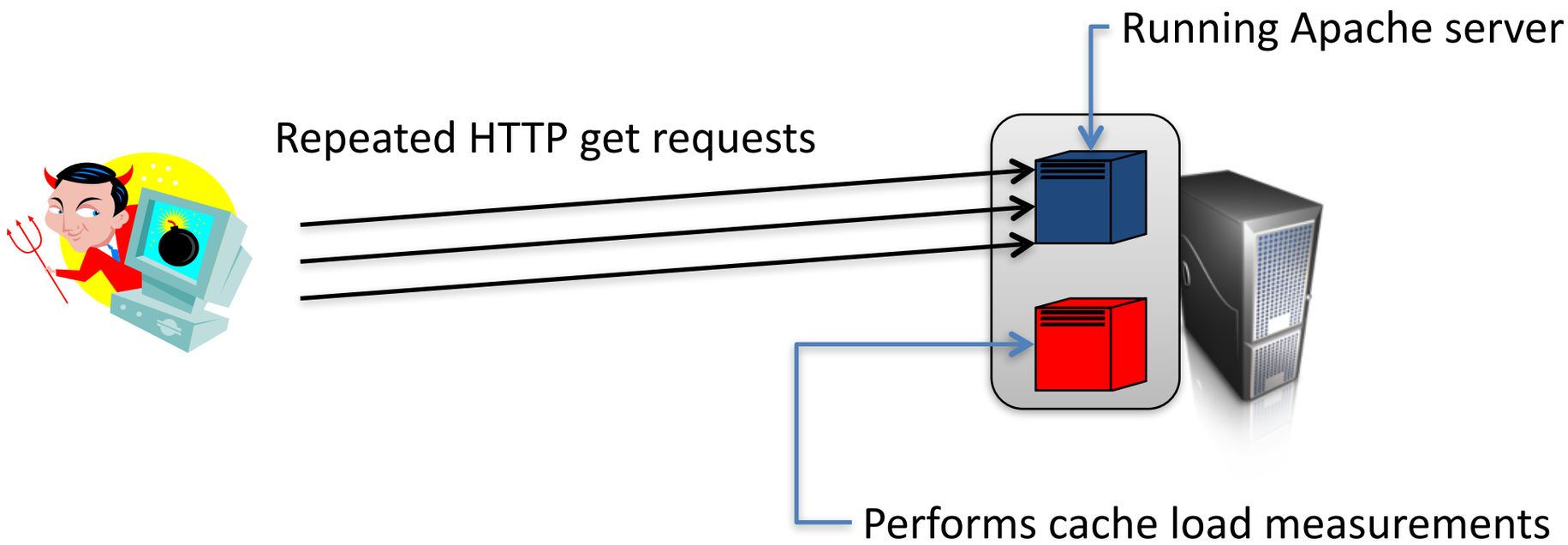


1) Read in a large array (fill CPU cache with attacker data)

2) Busy loop (allow victim to run)

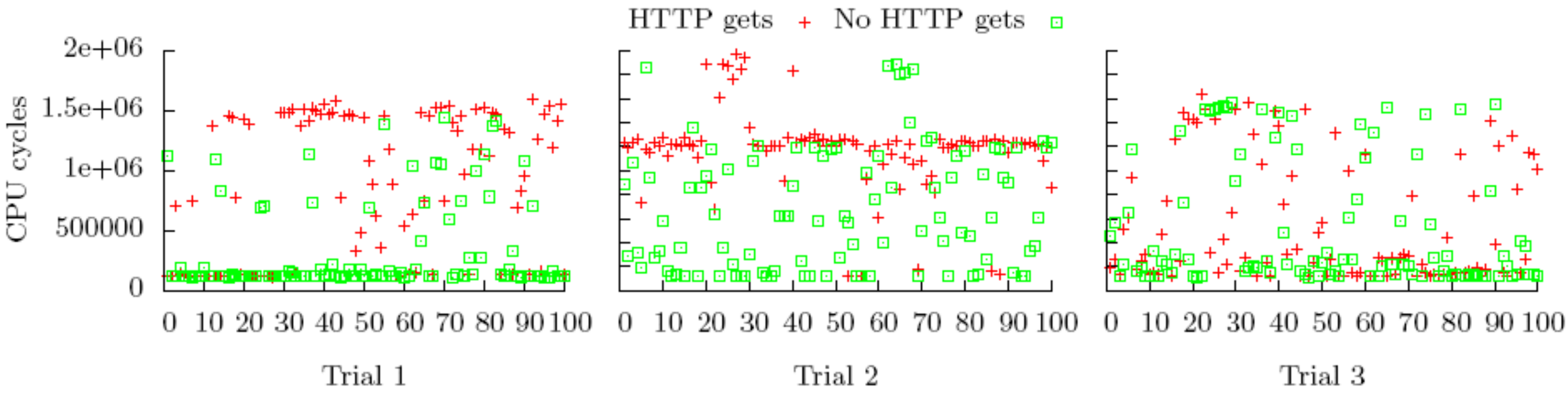
3) Measure time to read large array (the load measurement)

Cache-based cross-VM load measurement on EC2



3 pairs of instances, 2 pairs co-resident and 1 not

100 cache load measurements during **HTTP gets** (1024 byte page) and with **no HTTP gets**



[*Hey, You, Get Off of my Cloud*, 2009, Ristenpart, et al.]

recap

* Virtualization types, containment problems
* Linux RNG and reset vulnerabilities
* Cloud computing
  / Placement vulnerabilities
  / Co-residency detection via side-channels
  / Co-location strategies