Virtualization Wrap-up

CS642: Computer Security

Topics

- Side-channel wrap-up
- Leaked secrets

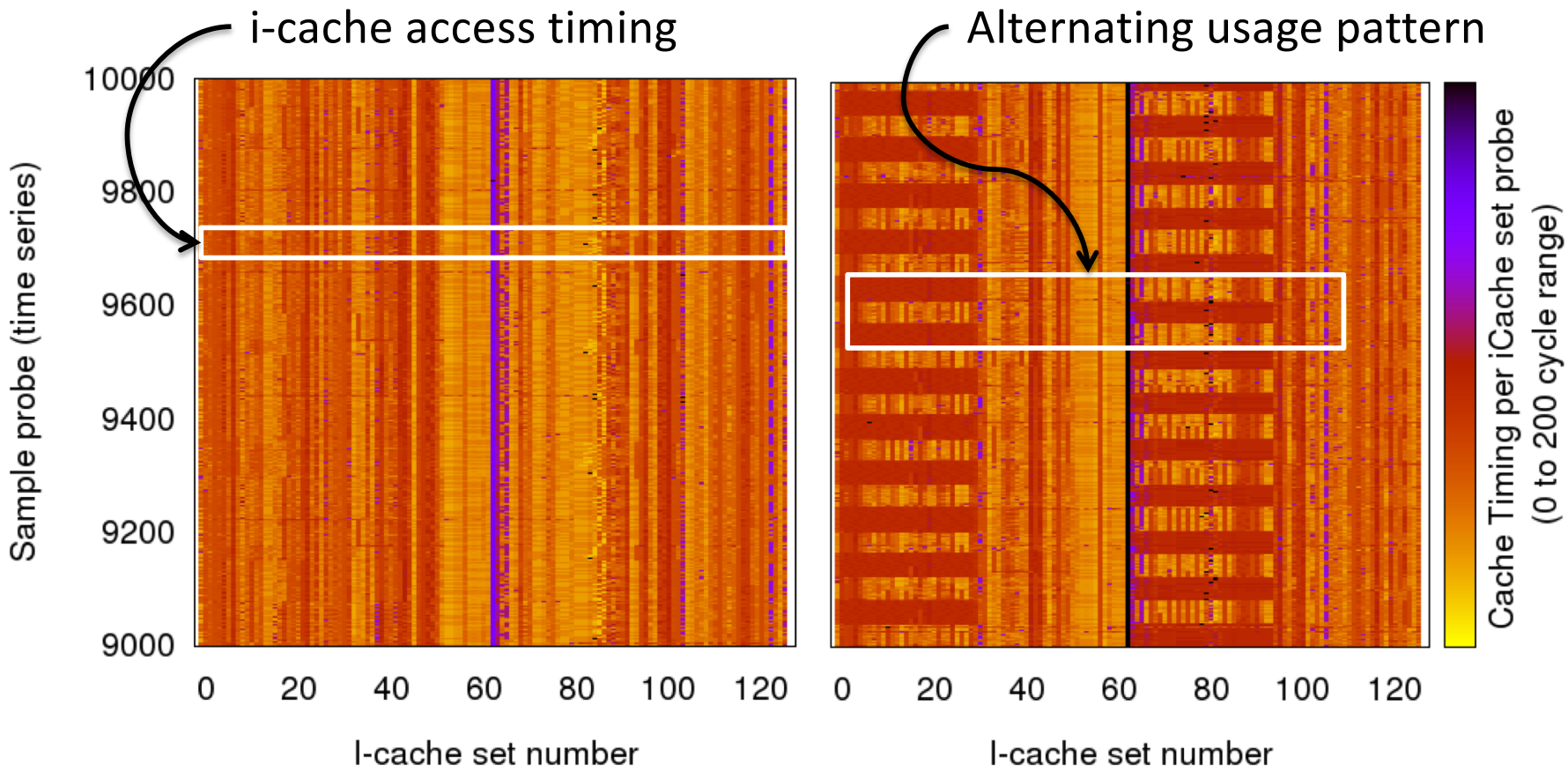
Side channel requirements

- What is needed for a side channel attack?
  - Shared hardware
    - Concurrent execution
  - Or shared hardware state
    - Rapid preemption
  - High-resolution timing

Side channel defenses

- Concurrent shared hardware
  - Hardware partitioning: dedicate core / socket per tenant
  - Migrate virtual machines to reduce concurrent sharing
- Shared hardware state
  - Flush state on context switch
- Rapid preemption
  - Limit frequency of preemption
- High-resolution timing
  - Fuzz timing

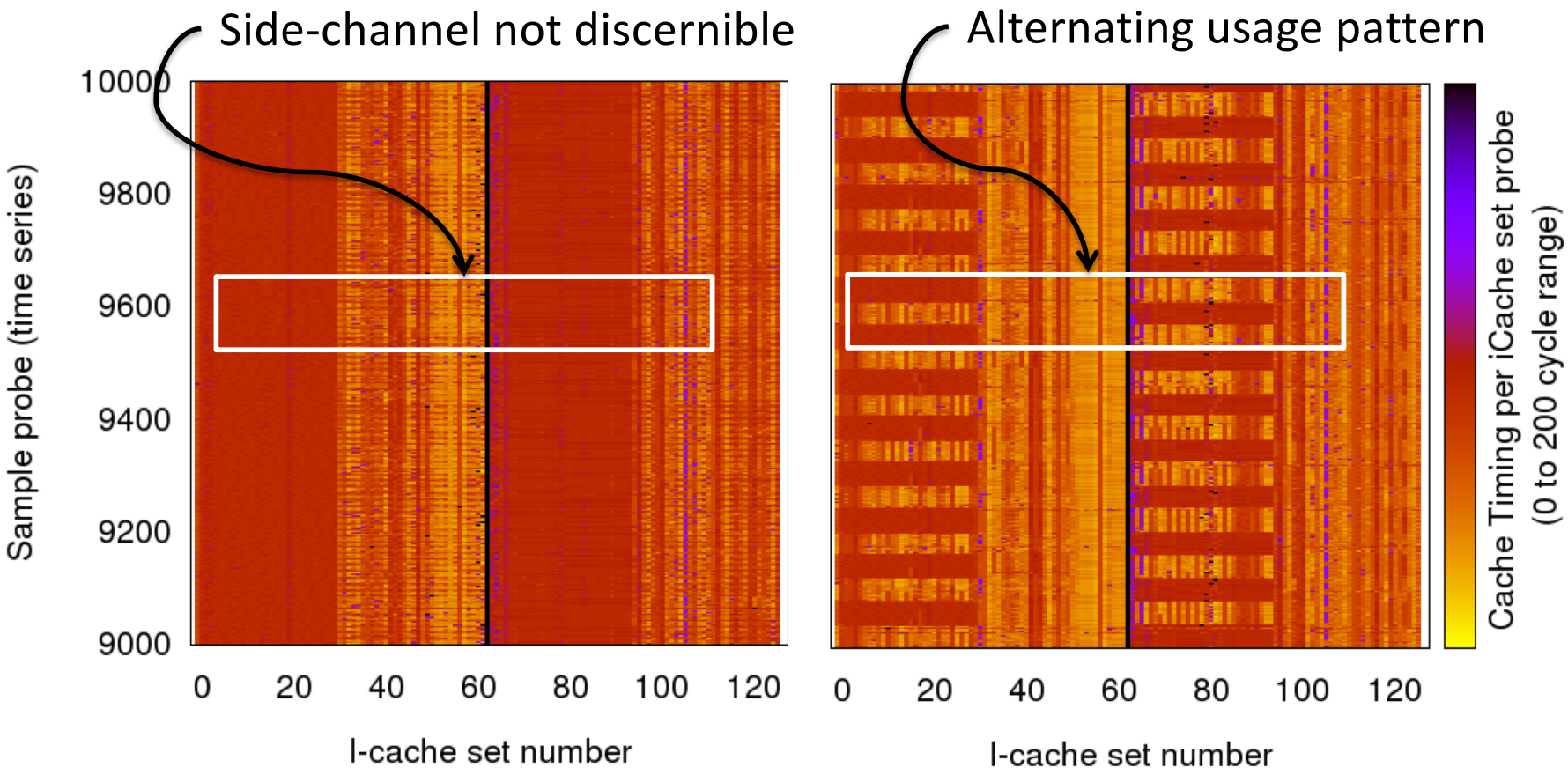
Security Evaluation : Prime-Probe Timing Profile



Idle Victim VM

Model Victim VM Under **Zero-MRT**

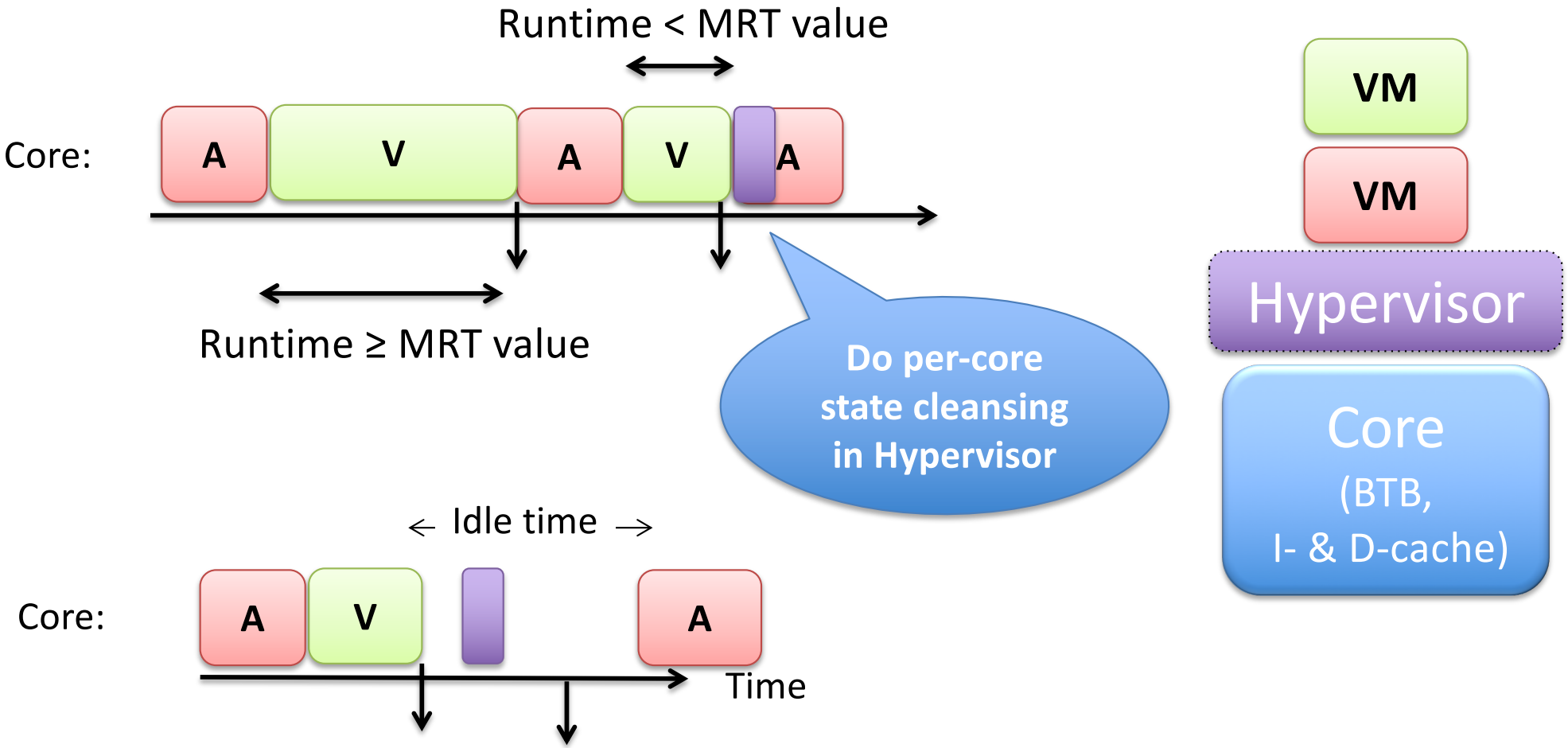
Security Evaluation : Prime-Probe Timing Profile



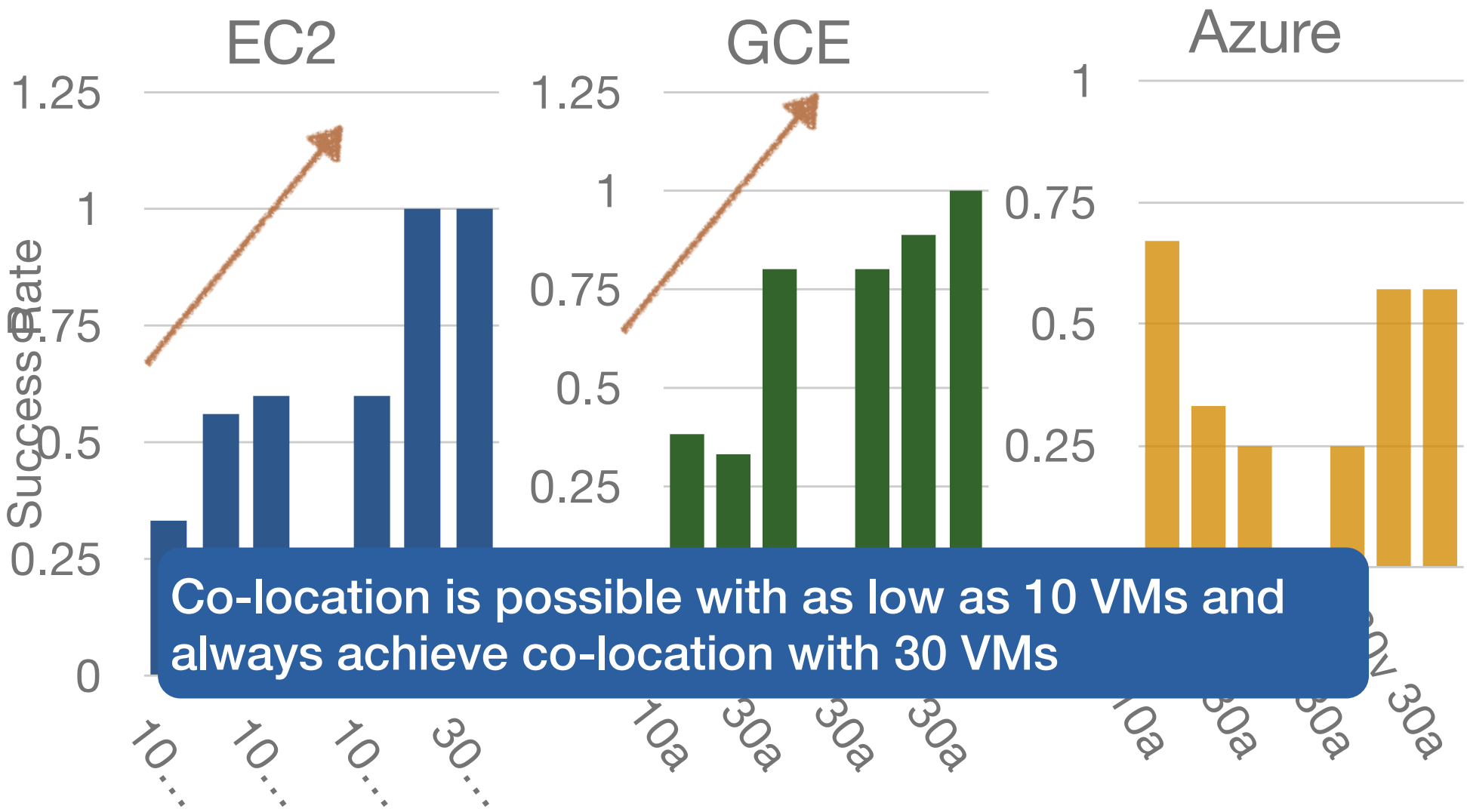
Model Victim VM Under **1ms MRT**

Model Victim VM Under **Zero-MRT**

Handling Interactive VMs: Per Core State Cleansing

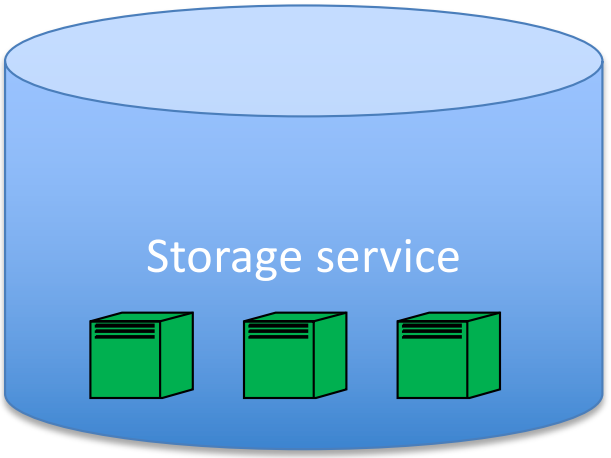


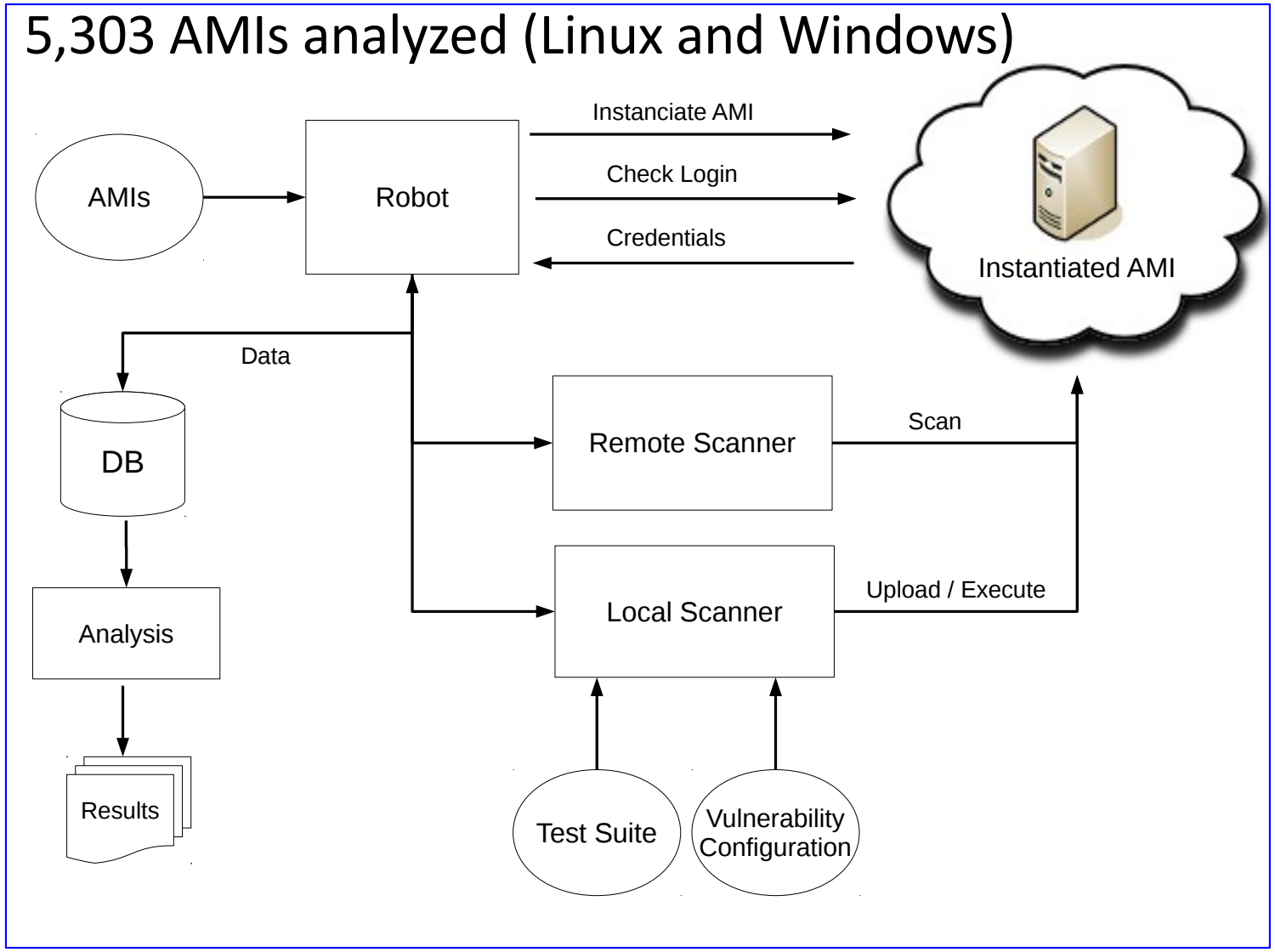
Results: Varying Number of VMs



Amazon Machine Images (AMIs)

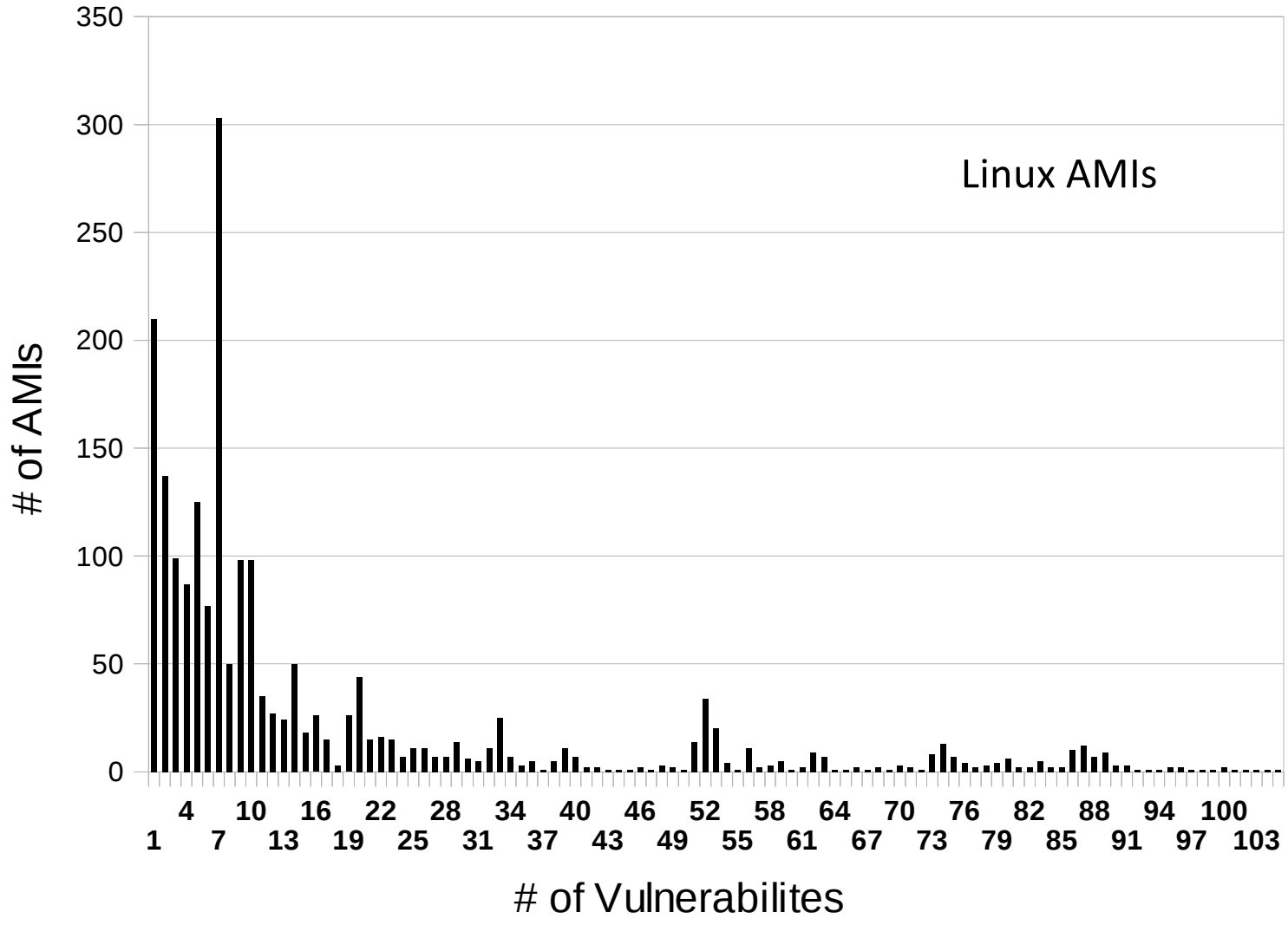
- Users set up volume snapshots / checkpoints that can then be run on the Elastic Compute Cloud (EC2)
- Can be marked as public and anyone can use your AMI





Balduzzi et al. “A Security Analysis of Amazon’s Elastic Compute Cloud Service – Long Version –”, 2011

See also Bugiel et al., “AmazonIA: When Elasticity Snaps Back”, 2011



Also: Malware found on a couple AMIs

Balduzzi et al. analysis

- Backdoors
  - AMIs include SSH public keys within authorized_keys
  - Password-based backdoors

	East	West	EU	Asia	Total
AMIs (%)	34.8	8.4	9.8	6.3	21.8
With Passwd	67	10	22	2	101
With SSH keys	794	53	86	32	965
With Both	71	6	9	4	90
Superuser Priv.	783	57	105	26	971
User Priv.	149	12	12	12	185

Table 2: Left credentials per AMI

Balduzzi et al. analysis

- Credentials for other systems
  - AWS secret keys (to control EC2 services of an account): 67 found
  - Passwords / secret keys for other systems: 56 found

Finding	Total	Image	Remote
Amazon RDS	4	0	4
dDNS	1	0	1
SQL	7	6	1
MySql	58	45	13
WebApp	3	2	1
VNC	1	1	0
Total	74	54	20

Table 3: Credentials in history files

Balduzzi et al. analysis

- Deleted files
  - One AMI creation method does block-level copying

Type	#
Home files (`/home, /root`)	33,011
Images (min. 800x600)	1,085
Microsoft Office documents	336
Amazon AWS certificates and access keys	293
SSH private keys	232
PGP/GPG private keys	151
PDF documents	141
Password file (`/etc/shadow`)	106

Table 5: Recovered data from deleted files

Response

"They told me it's not their concern, they just provide computing power," Balduzzi says. "It's like if you upload naked pictures to Facebook. It's not a good practice, but it's not Facebook's problem."

http://www.forbes.com/sites/andygreenberg/2011/11/08/researchers-find-amazon-cloud-servers-teeming-with-backdoors-and-other-peoples-data/

- Amazon notified customers with vulnerable AMIs
- Made private AMIs of non-responsive customers
- New tutorials for bundling systems
- Working on undelete issues…

Lessons

- New software management practices needed with VM snapshots
- Discussion:
  - New tool support?
  - How much worse is this than non-cloud server deployments?