

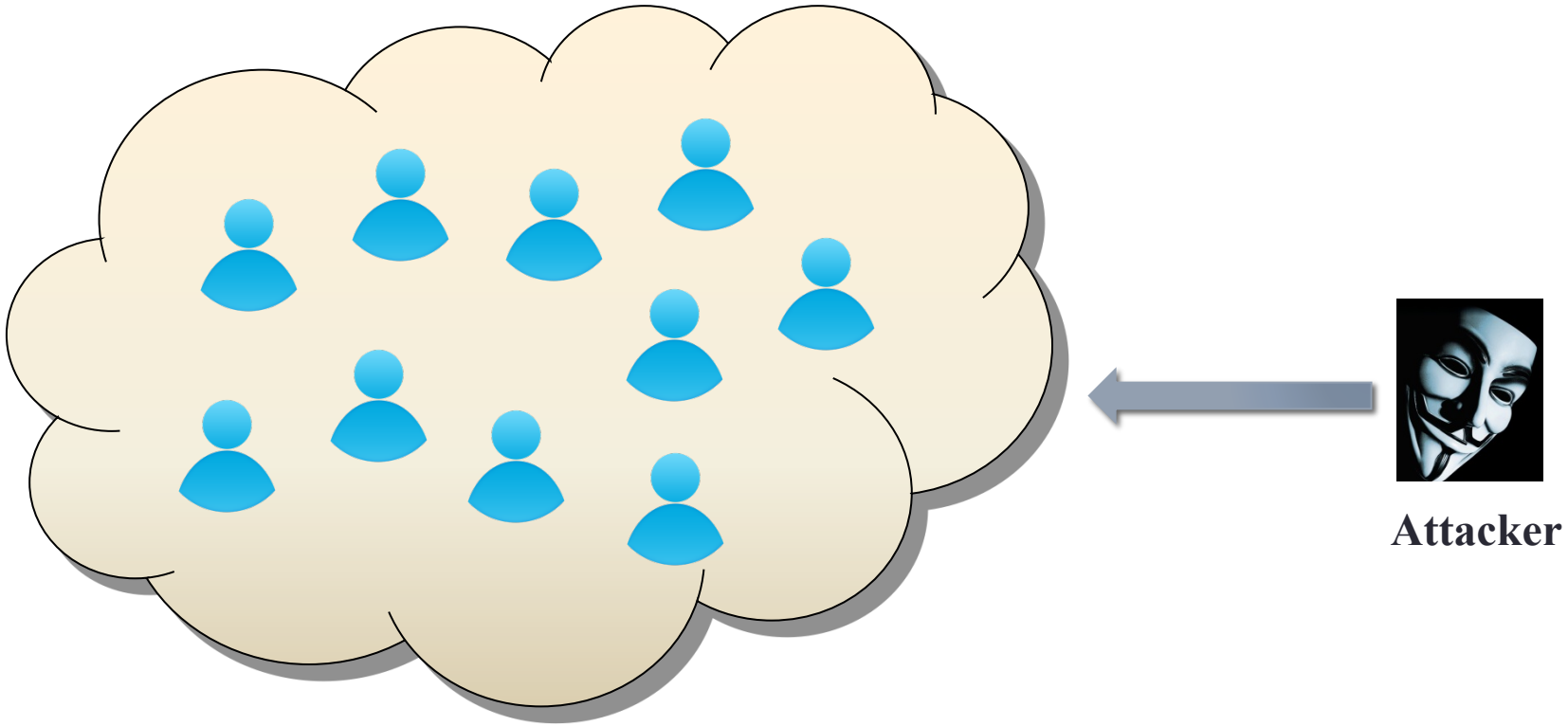


NEC Laboratories America
Relentless passion for innovation

A MEASUREMENT STUDY ON CO-RESIDENCE THREAT INSIDE THE CLOUD

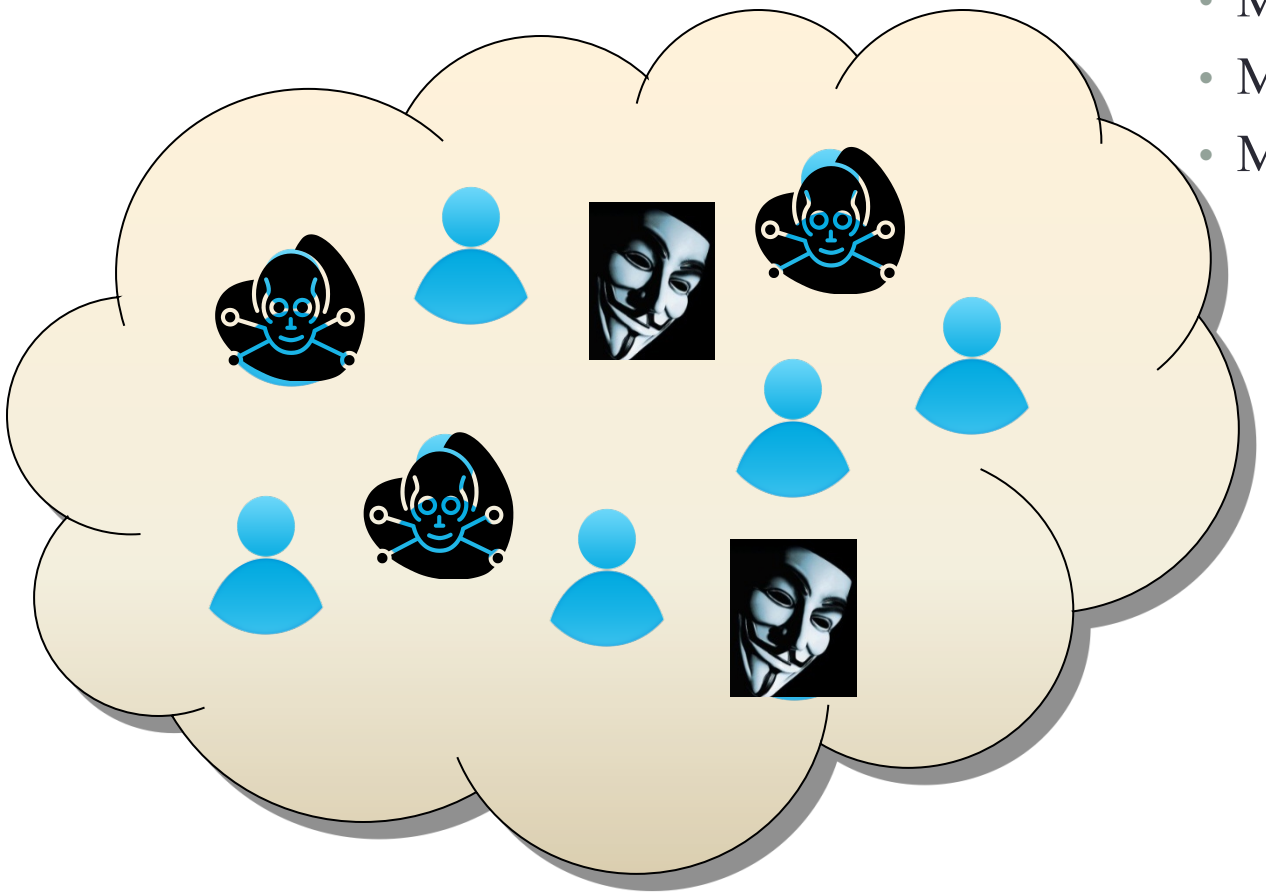
Zhang Xu — *College of William and Mary*
Haining Wang — *University of Delaware*
Zhenyu Wu — *NEC Laboratories America*

Cloud Becomes Tempting Target



- Valuable targets:
  - Banking, medical information, etc.
  - Enterprise sensitive information
  - Business competitor

Threats inside the Cloud

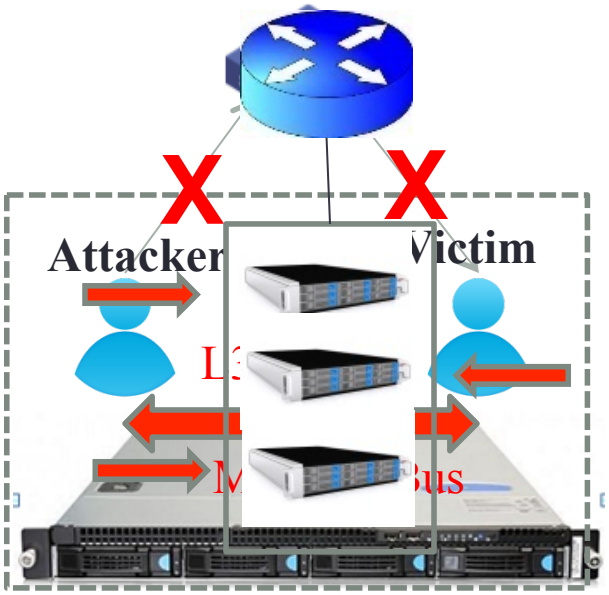


- Attack from inside
  - More victim information
  - More attack vectors
  - More stealthy

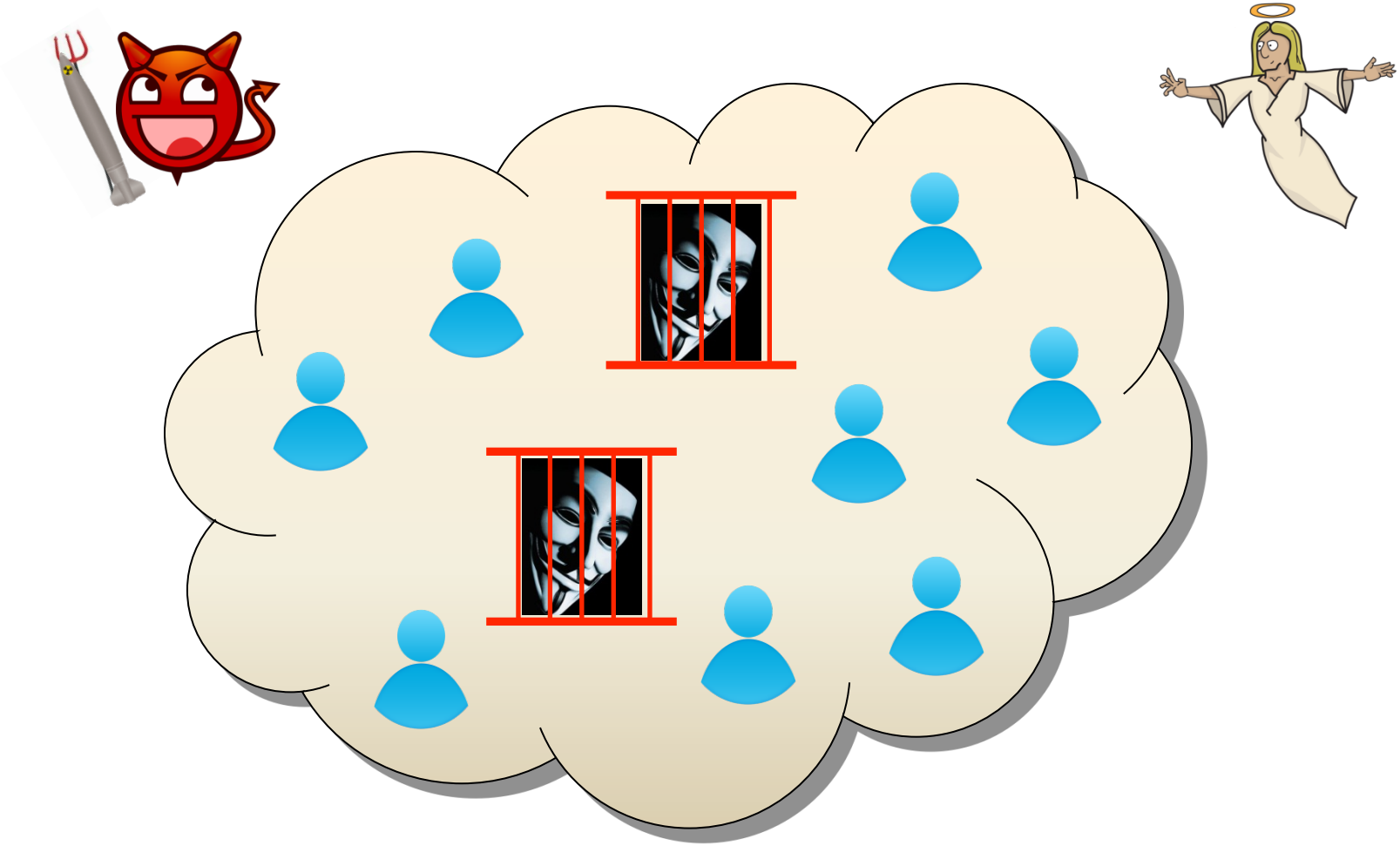
Co-residence Threats

- Co-residence:
  - *In a public multi-tenant cloud, several virtual machines/physical machines owned by different users are located in the same physical area*

- Attacks upon co-residence:
  - Machine level
    - VMs locating in the same physical machine
    - Covert channel
    - Side channel
  - Rack level
    - VMs locating in the same rack
    - Power attack



Understanding the Battle in Cloud



Our Measurement Study

- Quantify the co-residence inside the cloud.
- Understanding how cloud vendor adjusted VM placement policy and the impact on co-residence threat.
- Understanding how cloud vendor adjusted networking management with the impact on co-residence threat.
- Understanding co-residence threats in a defensive service: Virtual Private Cloud.

Amazon EC2

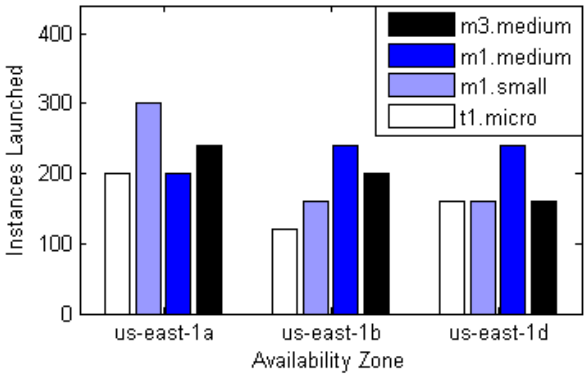
- Pioneer of Infrastructure as a Service with largest business scale
- Most businesses are held in US-east region (North Virginia)
- Instance type
  - t1.micro, m1.small, m3.large, …….
  - Indicate the "size" of the VM
  - Indicate the physical machine model hosting the instance
- Availability zones
  - "Logical" area in data center
  - 4 zones in us-east region: 1a, 1b, 1c, 1d

Our Measurement Study

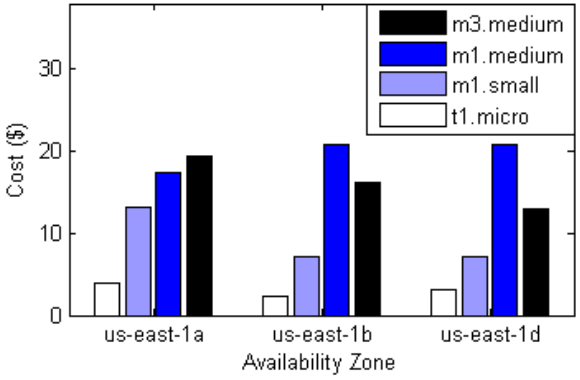
- Quantify the co-residence threat in the cloud.
- Understanding how cloud vendor adjusted VM placement policy and the impact on co-residence threat.
- Understanding how cloud vendor adjusted networking management and the impact on co-residence threat.
- Understanding co-residence threats in a defensive service: Virtual Private Cloud.

Co-residence Quantification

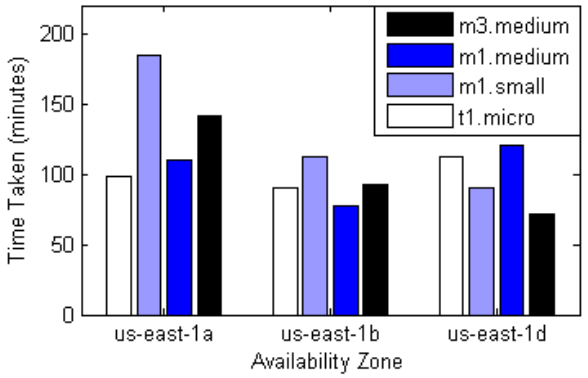
- Achieving random co-residence pair
  - Using two accounts to launch instances
  - Achieve any pair of co-residence instance



Number of instances required to achieve co-residence



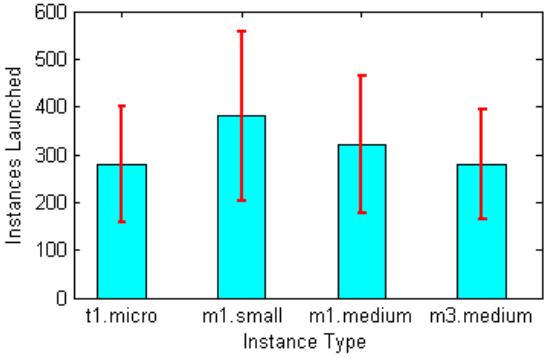
Money cost to achieve co-residence



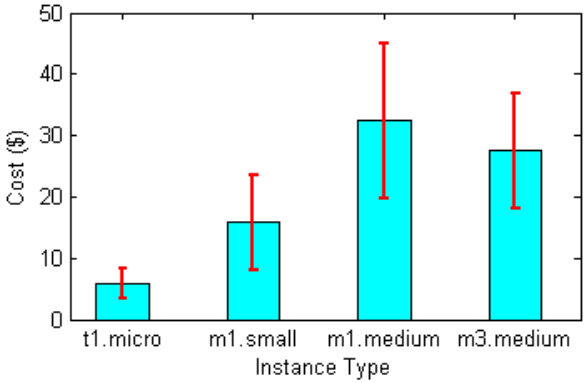
Time taken to achieve co-residence

Co-residence Quantification

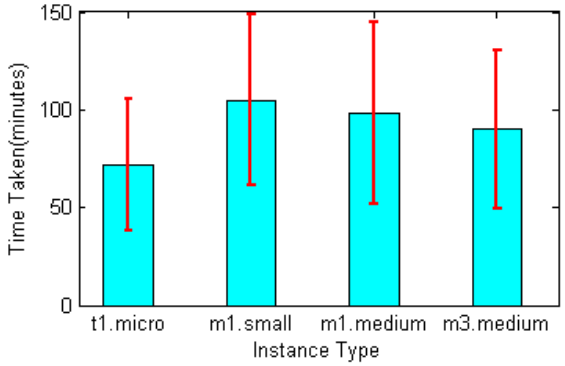
- Achieving co-residence with a target
  - Select a specific target
  - Achieve co-residence with the target



Number of instances required to achieve co-residence



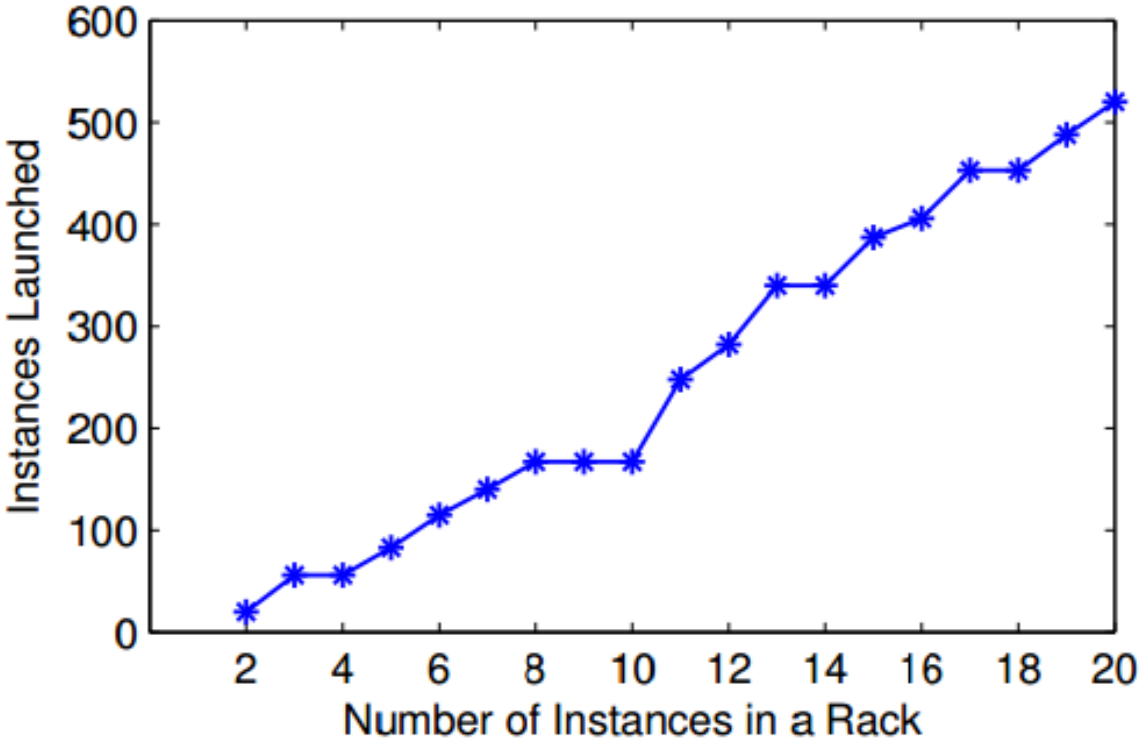
Money cost to achieve co-residence



Time taken to achieve co-residence

Co-residence Quantification

- Achieving rack-level co-residence
  - Leveraging ToR information (the first hop in trace-routing path)



Increasing Difficulty

- Compared with 2008 and 2012 results

2008
[Ristenpart'09]

	# victims v	# probes p	coverage
Zone 1	1	20	1/1
	10	20	5/10
	20	20	7/20
Zone 2	1	20	0/1
	10	18	3/10
	20	19	8/20
Zone 3	1	20	1/1
	10	20	2/10
	20	20	8/20

2012
[Wu'12]

2 random co-residence pairs with 160 probing instances

2014

More than 200 probing instances to get a random co-residence pair

Our Measurement Study

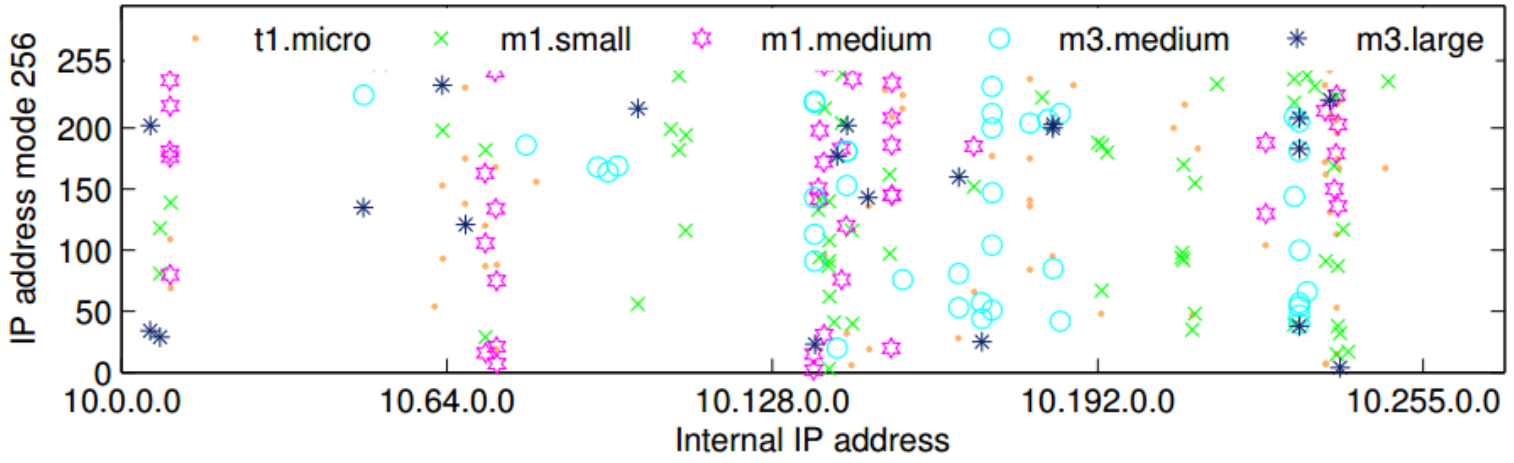
- Quantify the co-residence threat in cloud.
- Understanding how cloud vendor adjusted VM placement policy and the impact on co-residence threat.
- Understanding how cloud vendor adjusted networking management and the impact on co-residence threat.
- Understanding co-residence threats in a defensive service: Virtual Private Cloud.

Battle in VM placement

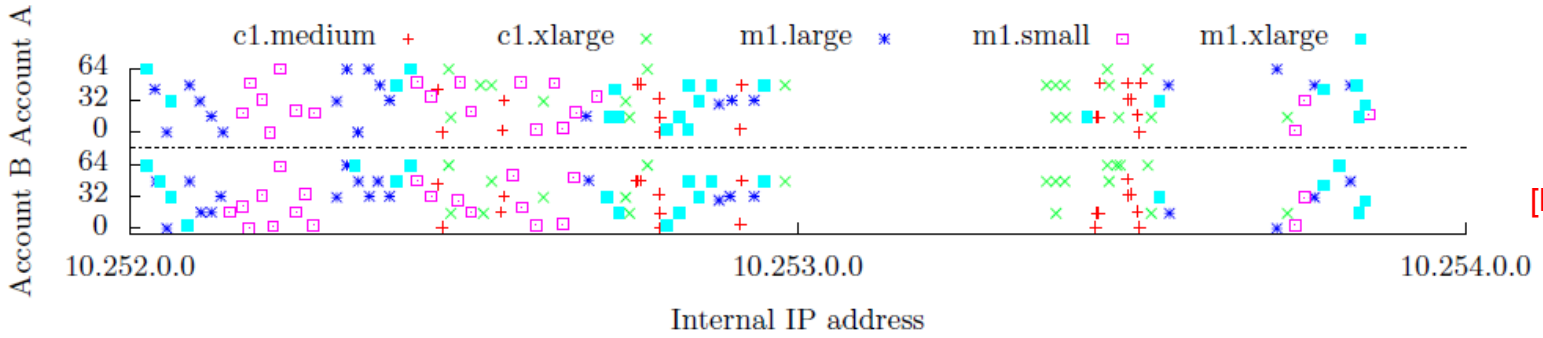
- Larger pool
  - **2008**: 1,785 m1.small instances on 87 physical machines
  - **2014**: 1,800 m1.small instances on 59 racks (at least 600 physical machines)
- Reduced placement locality

VM placement

- Location associated with instance type, i.e. type locality



2014

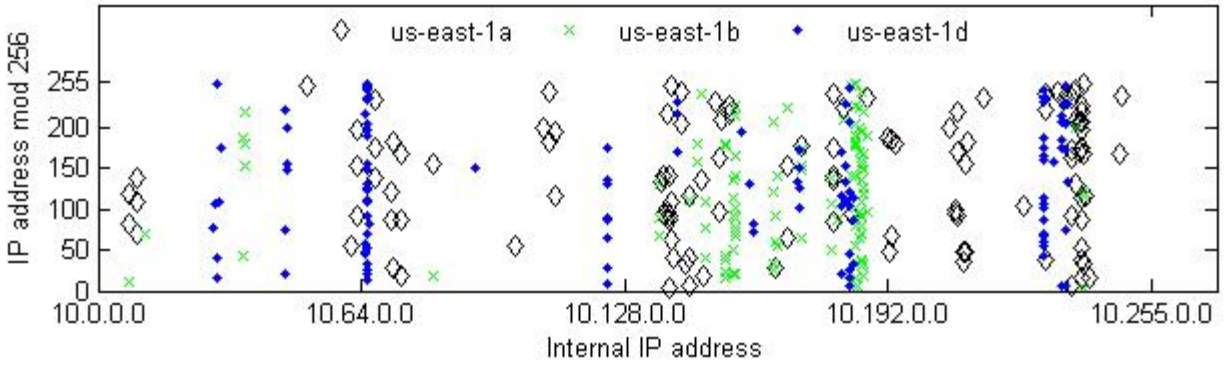


2008

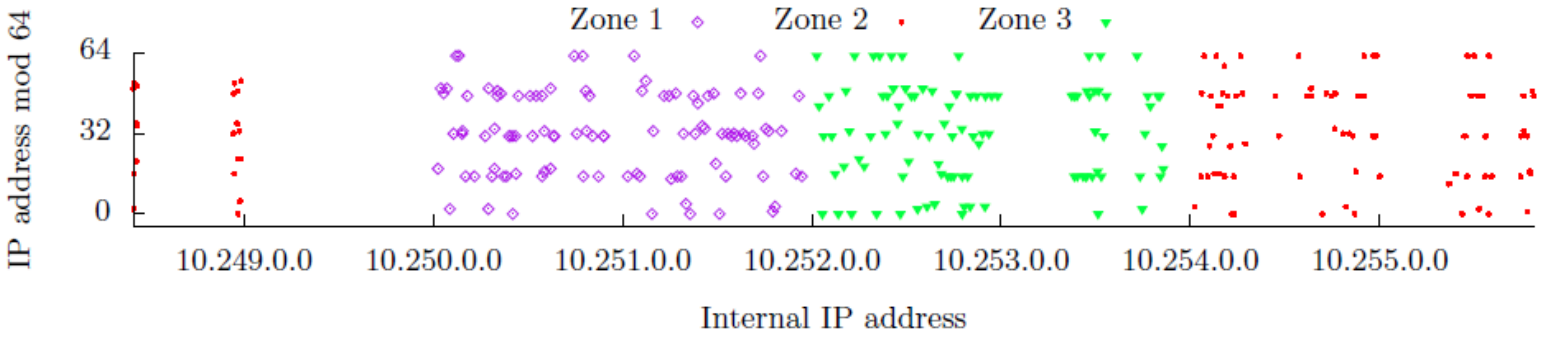
[Ristenpart'09]

VM placement

- Location associated with availability zones, i.e. zone locality



2014



2008

[Ristenpart'09]

Battle in VM placement

- Larger pool
  - **2008**: 1,785 m1.small instances on 87 physical machines
  - **2014**: 1,800 m1.small instances on 59 racks (at least 600 physical machines)
- Reduced placement locality
- More dynamic assignment
  - Public-private IP address mapping changes frequently
  - Different types of instances can be placed in same physical machine

Our Measurement Study

- Quantify the co-residence threat in cloud.
- Understanding how cloud vendor adjusted VM placement policy and the impact on co-residence threat.
- Understanding how cloud vendor adjusted networking management and the impact on co-residence threat.
- Understanding co-residence threats in a defensive service: Virtual Private Cloud.

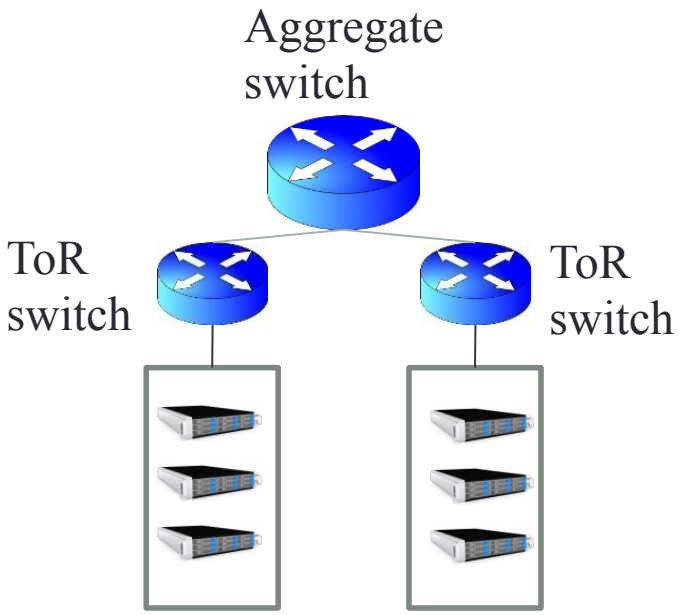
Networking Management

- Measurement methodology
  - Trace-routing from multiple sources to random instances in EC2
  - Trace-routing among controlled instances
  - "*Neighborhood trace-routing*"
    - From a source instance, perform trace routing to all those instances that share /23 prefix of their private IP addresses with our source instances

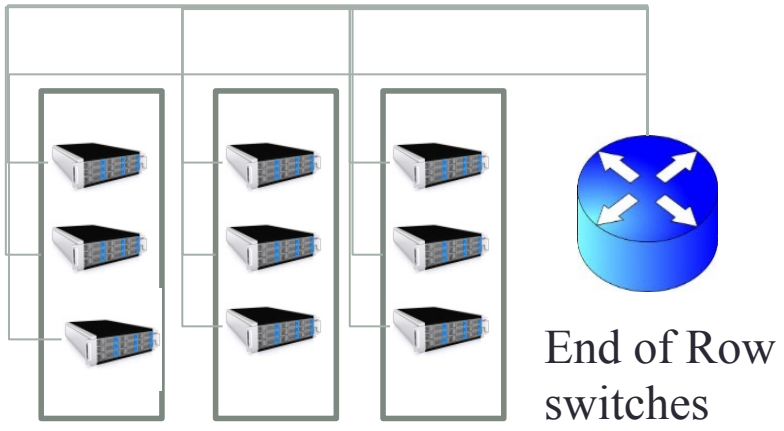
Networking Management

- Hidden Domain0
  - Domain0 is the identifier of the physical machine
  - Hiding Domain0 in routing path significantly increases difficulty to achieve co-residence
- Hidden hops in routing paths
  - Important routers and switches no longer appear in trace-routing paths
    - In 2013 all paths are even-hop [Lacurts'13]
    - 34.26% of all paths have odd-hop
  - 76.11% of paths have at least one hop obscured (filled with stars)

Networking Topology



Top of Rack Topology



End of Row Topology

Identifying Networking Topology

- Two “generations" of instances
  - The old generation: all the instances with m1 type
  - the new generation: all other types
- 109 racks identified
  - 77 old generation racks
  - 32 new generation racks
- 14 racks are non-ToR connected
  - 12 old generation racks
  - 2 new generation racks
- ToR topology is dominating and is the trend
  - More vulnerable to rack level co-residence threats!

Our Measurement Study

- Quantify the co-residence threat in cloud.
- Understanding how cloud vendor adjusted VM placement policy and the impact on co-residence threat.
- Understanding how cloud vendor adjusted networking management and the impact on co-residence threat.
- Understanding co-residence threats in a defensive service: Virtual Private Cloud.

Virtual Private Cloud (VPC)

- VPC is a service to enhance cloud security
  - Provides an isolated networking environment to host instances
  - Private address is invisible to others
  - Help to suppress co-residence

- VPC is widely used in EC2
  - All instances in VPC have public IP addresses in 5 IP ranges.

Co-residence in VPC

- Network is isolated, but physical resources may still be shared!
  - Co-residence is still possible
- Challenge: very limited network information
  - No private address
  - Routing information is obscured

```
Traceroute to 54.91.46.65 (54.91.46.65), 30 hops max, 60 byte packetes
1  * * *
2  * * *
3  100.64.37.82 (100.64.37.82) 14.573 ms   100.64.36.82 (100.64.36.82)  14.813 ms
4  10.1.172.197 (10.1.172.197) 14.734 ms   10.1.32.195  (10.1.32.195)   14.828  ms
5  10.1.14.6 (10.1.14.6)  14.976 ms  14.708 ms   10.1.16.6 (10.1.16.6)  14.849 ms
6  ec2-53-91-46-65.compute-1.amazonaws.com (54.91.46.65)  14.898 ms   0.942 ms
```

```
Traceroute 54.88.197.86 (54.88.197.86), 30 hops max, 60 byte packets
1  10.210.136.3 (10.210.136.3) 1.248 ms  1.303 ms  1.501 ms
2  ip-10-1-14-17.ec2.internal (10.1.14.17)  0.529 ms  0.653 ms  0.781 ms
3  ip-10-1-172-2.ec2.internal (10.1.172.2)  0.492 ms  0.604 ms  0.729 ms
4  * * *
5  * * *
6  ec2-54-88-197-86.compute-1.amazonaws.com (54.88.197.86)  1.048 ms  0.883 ms
```

Co-residence in VPC

- Key: number of hops in routing paths and latency are not hidden!

- Use latency to speculate the type and availability zone of target
  - The latency between instances with different types in different zones have certain pattern
  - Launch probing instances with same type in same zone

Co-residence in VPC

Anchor Instance in EC2 default network

	1a-t1.micro	1a-m1.small	1a-m1.medium	1b-t1.micro	1b-m1.small	1b-m1.medium
1a-t1.micro	1.224ms	1.123ms	1.025ms	2.237ms	2.221ms	2.304ms
1a-m1.small	1.361ms	1.059ms	1.100ms	2.208ms	2.055ms	2.198ms
1a-m1.medium	1.165ms	1.102ms	0.986ms	2.211ms	2.060ms	1.988ms
1b-t1.micro	2.101ms	2.235ms	2.188ms	1.108ms	1.243ms	1.202ms
1b-m1.small	2.202ms	2.003ms	2.190ms	1.131ms	0.968ms	1.048ms
1b-m1.medium	2.087ms	2.113ms	1.965ms	1.088ms	1.023ms	0.855ms

Instance in VPC

Latency vector



1.221ms	1.146ms	1.011ms	2.537ms	2.233ms	2.404ms

77.8% accuracy

Co-residence in VPC

- Key: number of hops in routing paths and latency are not hidden!

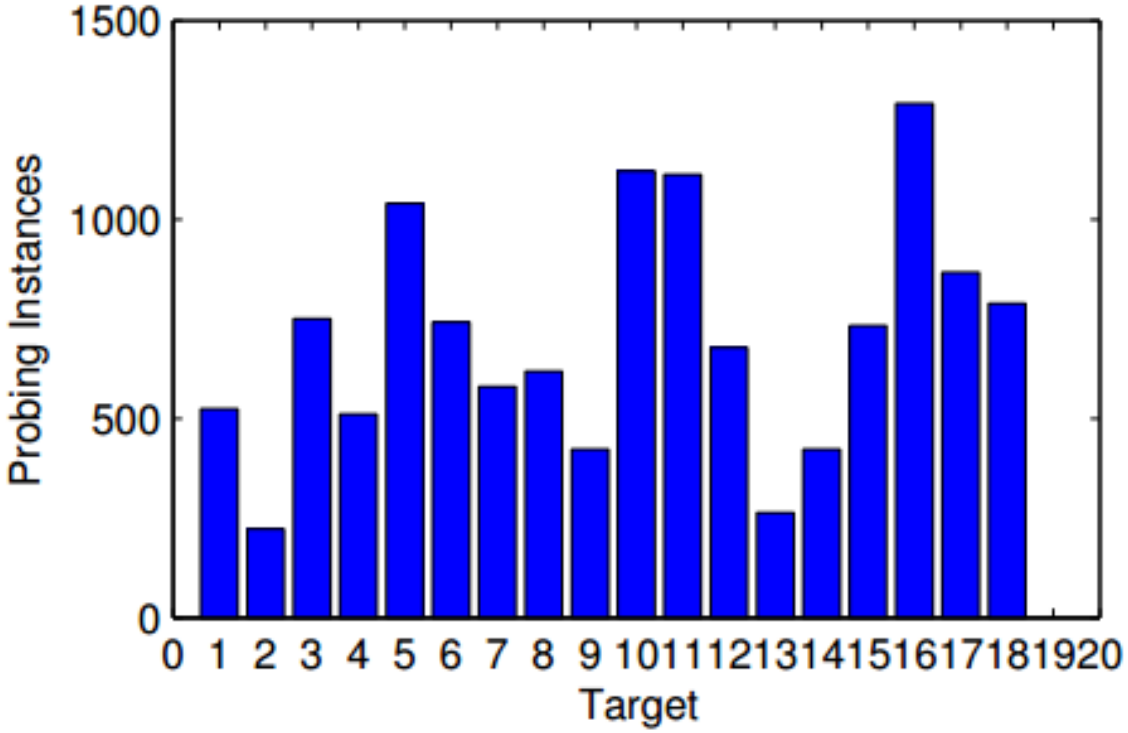
- Use latency to speculate the type and availability zone of target
  - The latency between instances with different types in different zones have certain pattern
  - Launch probing instances with same type in same zone

- Use number of path hops and latency to filter non-co-residence pairs
  - Co-residence instances should have same number of hops to same target
  - Latency between co-residence pairs should be below certain threshold

Co-residence in VPC

- The target and our probing attack instance should share the same number of hops to all of our anchor instances.
  - Filter out 63.2% candidates
- The end-to-end latency from probing instance and target should be below certain threshold.
  - Filter out 97% candidates
- Use covert channel to verify co-residence
  - 17.6% of instances that pass the two-steps filtering really achieve co-residence

Co-residence in VPC



Effort to achieve co-residence with target in VPC

- VPC increases difficulty of achieving co-residence significantly
- VPC cannot eliminate the co-residence threat

More Secure Cloud Management

- Manage naming system properly
  - Introduce randomness
- Not publish public IP address range
- Protecting routing information
- Introduce more dynamic VM placement policy
  - Leverage user historical information

Conclusion

- Our work demonstrates that EC2 has adjusted VM placement policy, which makes co-residence attack more difficult.
- Our measurement shows how networking management adjustment can help mitigate co-residence threat.
- Our study proves the effectiveness of VPC, but even with VPC, co-residence threat still exists in cloud.

Thank You

Questions?