T. Ristenpart *et al.*

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds

(ACM CCS 2009)

Yang Tang

Sept. 14, 2011

Some slides are adapted from the course: http://www.cse.cuhk.edu.hk/~tangyang/cmsc5709

Cloud computing

In cloud computing, users can instantiate virtual machines (VMs) on demand for computation

You pay for the resources that you need:

CPU? Memory? Storage?

Virtualization

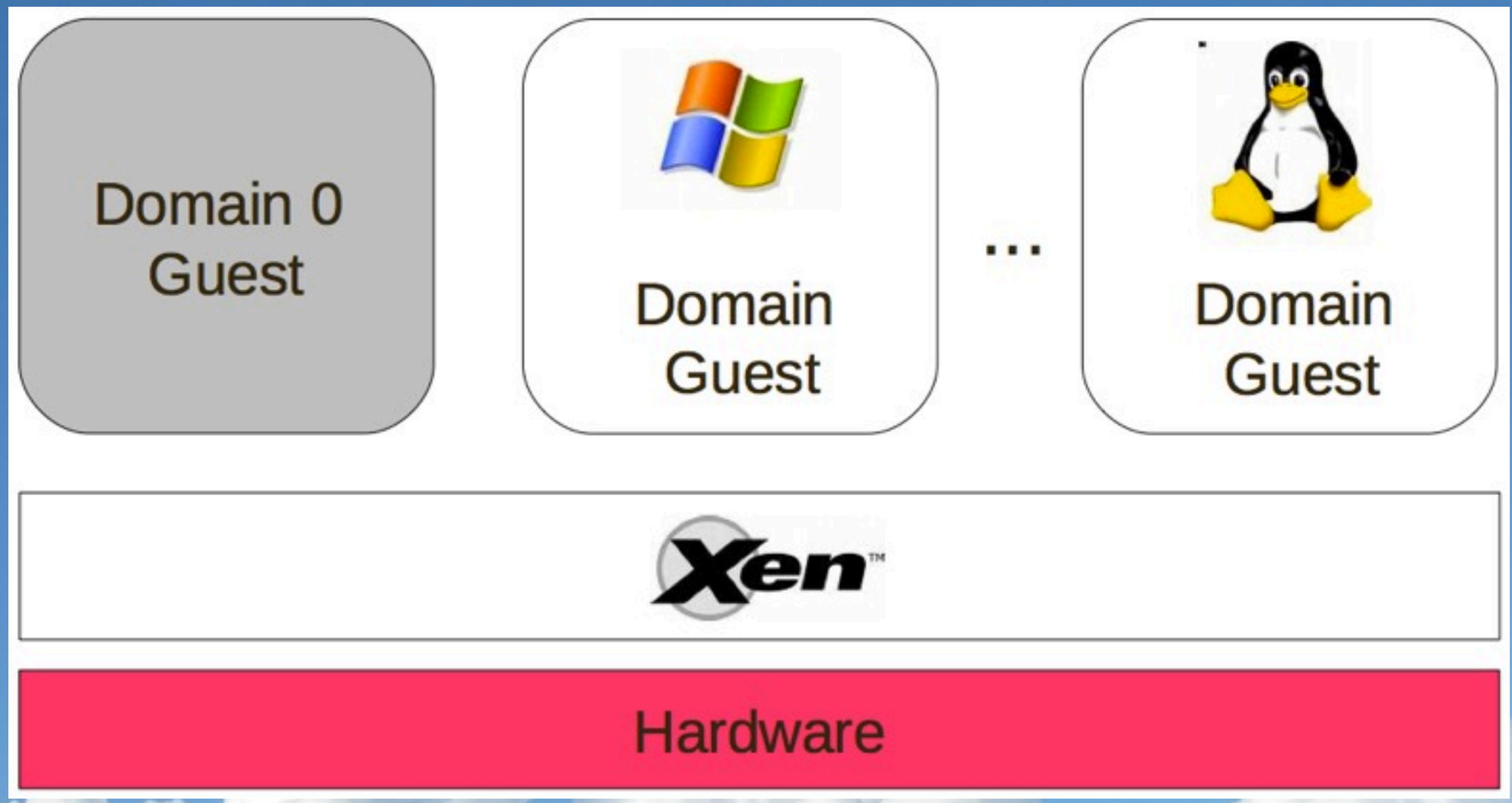
A virtual machine is treated like a physical server on which you can run services (e.g., Apache)

Idea of virtualization:

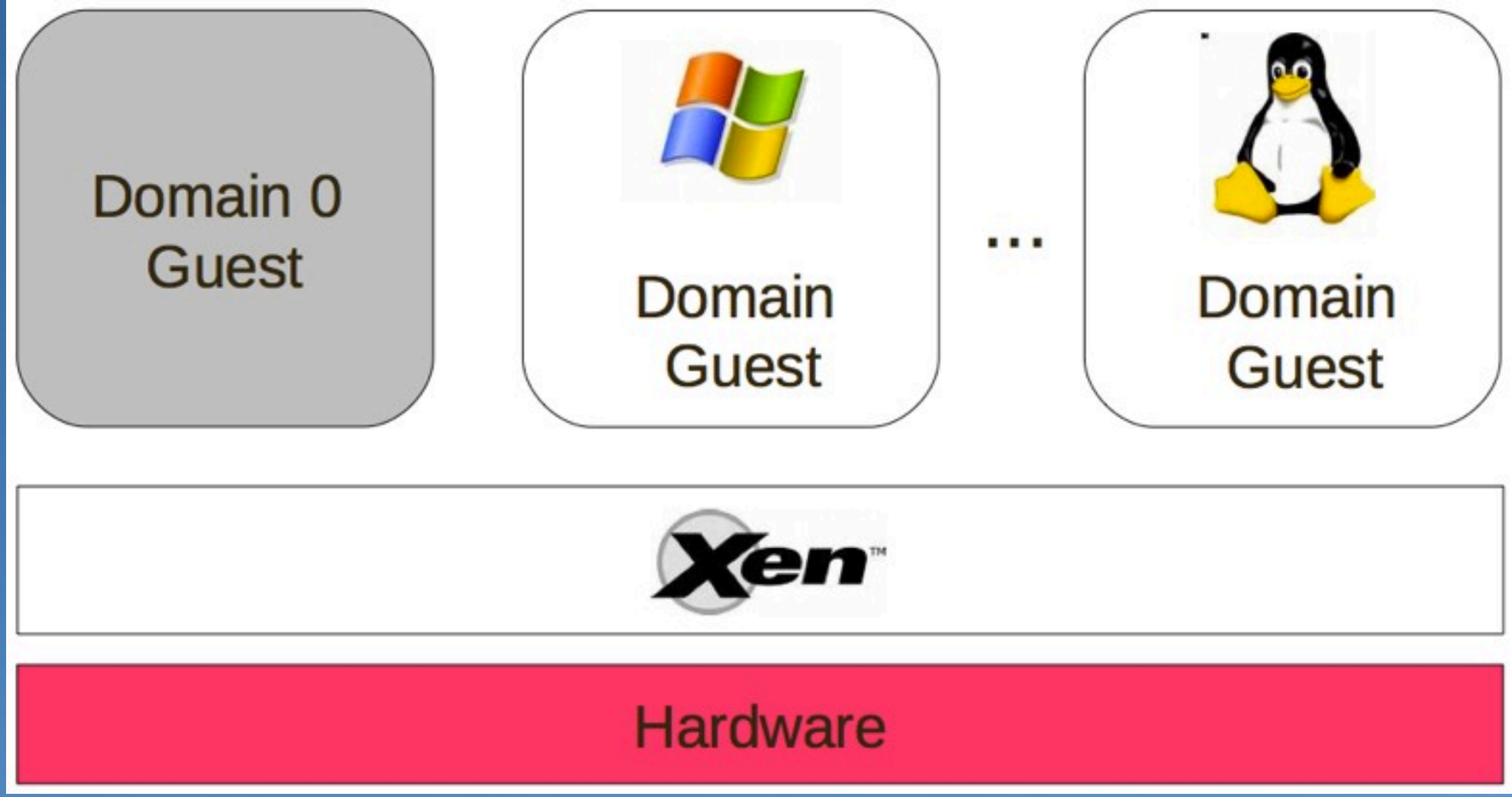
multiplexing many customer VMs across a shared physical infrastructure

EC2 backgrounds

Amazon EC2 uses Xen to monitor VMs



Source: http://xen.org/files/Marketing/NewtoXenGuide.pdf



Dom0: a privileged VM that manages guest images, their physical resource provisioning, and any access control rights

Source: http://xen.org/files/Marketing/NewtoXenGuide.pdf

EC2 backgrounds

Each running VM image is called an instance

As in 2009, Amazon provides 2 regions (US/EU); each has 3 availability zones with separate power and connectivity

A user can specify the region and the availability zone to run an instance

EC2 backgrounds

A user can specify an instance type (computational power, memory, storage space)

For example:

"m1.small": 1 ECU (1.0-1.2GHz CPU), 1.7GB RAM, 160GB storage

"m1.large": 2 ECUs, 7.5GB RAM, 850GB storage

EC2 backgrounds

Each instance has an external IP and an internal IP

For example:

external IP: 75.101.210.100

internal IP: 10.252.146.52

Given an external IP, we can use DNS queries to get its internal IP

Why cloud computing brings new threats?

Traditional system security mostly means keeping bad guys out

The attacker needs to either compromise the authorization system, or impersonate existing users

But cloud allows multi-tenancy:

multiple independent users share the same physical infrastructure

Threat model

A customer's VM could be assigned to the same physical server as the adversary's VM

The adversary's VM can steal information of the customer's VM via physical shared resources

Two attacks

Placement

the adversary arranges to place their VMs on the same physical machine used by their target customers

Extraction

the adversary extracts confidential information via a cross VM attack

Attacker's challenges

How to find out where the target is located

How to be co-resident with the target in the same physical machine

How to gather information about the target

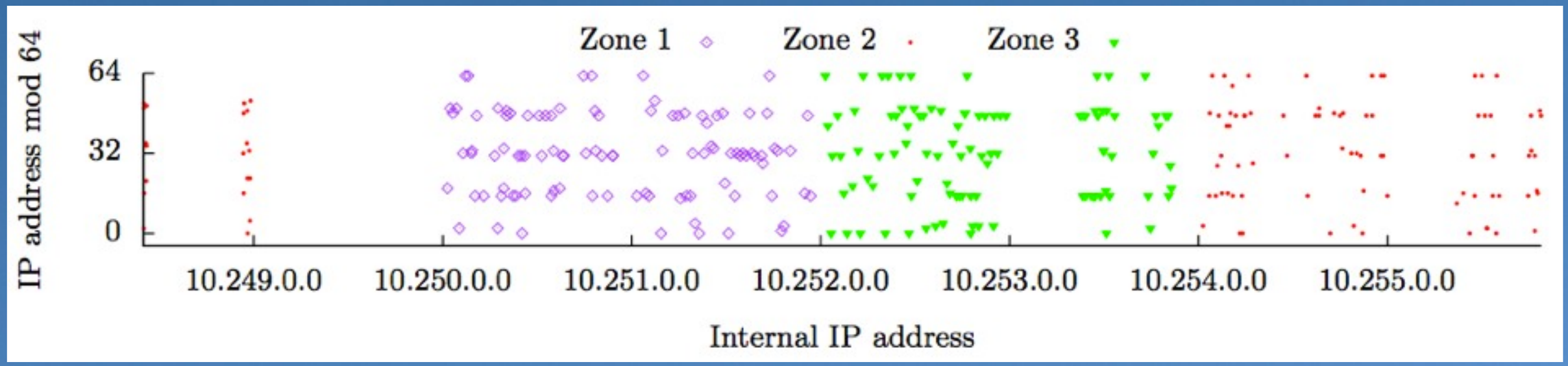
Contributions

Shows the practicality of placement and extraction attacks on a commercial cloud Amazon EC2

- determine where an instance is located
- determine if two instances are co-resident
- launch instances co-resident with the target instance
- exploit cross-VM information leakage

40% success in achieving co-residence with target VM

Cloud cartography

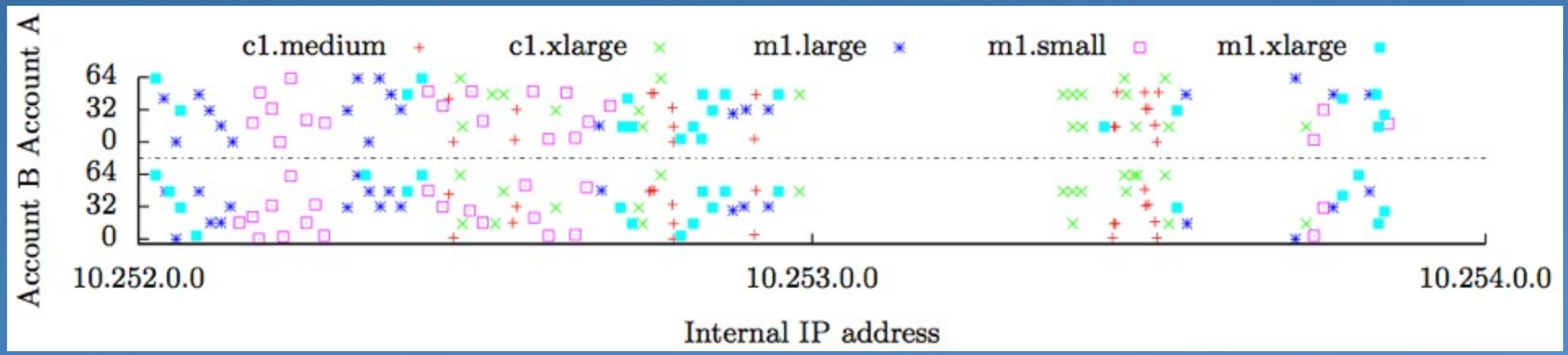


Each availability zone seems to use a range of internal IPs

Internal IPs are statically assigned

All IPs from a /16 prefix are from the same zone

Cloud cartography



"same instance type" + "same zone" = "similar IP regions"

Most /24 prefixes have one instance type

Determining co-residence

If two instances have...

Matching Dom0 IP address (determined by traceroute)

small packet RTT

numerically close internal IP addresses

Placement attack

Goal: launch a malicious VM co-resident with target

Observation 1: a single account won't have two instances running on the same physical machine

Strategy 1 (brute-force):

Enumerates a set of potential target victims

Apply co-resident checks for verification

Placement attack

Observation 2 (parallel locality): if two accounts run two instances at the same time, then they are likely on the same machine

Strategy 2 (instance flooding):

Run a lot of instances in parallel as soon as the target VM launches

Placement attack

How can we know if the target VM is just launched?

In cloud computing, server runs on demand

An attacker can probe the target server regularly, wait until it disappears and reappears

Success rate: 40%

Extraction attack

Now that an attacker can achieve co-residence, what can it do with the target VM?

- Measuring cache usage
- Estimating traffic rates
- Keystroke timing attack
- Any possible side-channel attacks -- you imagine!

How to defend...

...against cartography and co-resident checks?

Use randomized IP addresses
Block tools such as traceroute

...against placement attacks?

Let users choose where to place VMs

...against extraction attacks?

Use blinding techniques

A better strategy: avoid co-residence at all!

Class discussion

How is the security problem different from other attacks?

What is so special about clouds?

Given the current EC2 implementation, what would you do in order to protect yourself?

Background photo credit: stock.xchng #1289343