THE EC2 SERVICE

THE EC2 SERVICE

- Amazon's Elastic Compute Cloud
- Provide computational resources
- EC2 provides the ability to run
  - Linux
  - FreeBSD
  - OpenSolaris
  - Windows as guest operating systems
- Xen hypervisor
  - Virtual machine monitor
  - Provides isolation between VMs, intermediating access to physical memory and devices.

Privileged Virtual Machine

- Called Domain0 (Dom0) in the Xen, is used to
  - Manage guest images
  - Physical resource provisioning
  - Access control rights.

- In EC2 the Dom0 VM is configured to route packets for its guest images and reports itself as a hop in traceroutes.

Registration with EC2

- User creates an account uniquely specified by its contact e-mail address
- Provides credit card information for billing
- With a valid account
  - user creates one or more VM images
- Running image is called an instance
- When the instance is launched
  - Assigned to a single physical machine within the EC2 network for its lifetime
- EC2 does not support live migration of instances, although this should be technically feasible.
- By default, each user account is limited to 20 concurrently running instances.

Amazon provides two “regions”

- One located in the United States & one in Europe.
- Each region contains three “availability zones” which are meant to specify infrastructures with distinct and independent failure modes (e.g., with separate power and network connectivity).
- When requesting launch of an instance, a user specifies the region and may choose a specific availability zone (otherwise one is assigned on the user’s behalf).

Instance Type

- Combination of computational power, memory & persistent storage space available to the virtual machine.
- Five Linux instance types
  - m1.small
  - c1.medium
  - m1.large
  - m1.xlarge
  - c1.xlarge
- The first two are 32-bit architectures, the later three are 64-bit.

- Small compute slot (m1.small)
  - Single virtual core providing one ECU (EC2 Compute Unit
  - Claimed to be equivalent to a 1.0–1.2 GHz 2007 Opteron or 2007 Xeon processor)
  - 1.7 GB of memory and 160 GB of local storage

- Large compute slot (m1.large)
  - Provides 2 virtual cores each with 2 ECUs,
  - 7.5GB of memory and 850GB of local storage.

Charges

- ‘m1.small’ in the United States region is currently $0.10 per hour,
- ‘m1.large’ is currently $0.40 per hour

- Given these constraints, virtual machines are **placed on available physical servers** shared among multiple instances.

- Each instance is given **Internet connectivity** via both an **external IPv4 address** and domain name and an **internal private address** and domain name.

- For example, an instance might be assigned
  - external IP 75.101.210.100,
  - external name ec2-75-101-210-100.compute-1.amazonaws .com
  - internal IP 10.252.146.52
  - internal name domU- 12-31-38-00-8D-C6.compute-1.internal.

- Within the cloud, both domain names resolve to the internal IP address; outside the cloud the external name is mapped to the external IP address.

NETWORK PROBING

- External probes and internal probes
- A probe is external when it originates from a system outside EC2 and has destination an EC2 instance.
- A probe is internal if it originates from an EC2 instance and has destination another EC2 instance.
- DNS resolution queries to determine the external name of an instance and also to determine the internal IP address of an instance associated with some public IP address.
- The later queries are always performed from an EC2 instance.

Cloud Security

- Customers must trust their cloud providers to respect the privacy and integrity of their data and computation.

- it is conceivable that a customer's VM could be assigned to the same physical server as their adversary.

- Adversary might penetrate the isolation between VMs (e.g., via a vulnerability that allows an "escape" to the hypervisor or via side-channels between VMs) and violate customer confidentiality

Two main steps: placement and extraction.

- Placement refers to the adversary arranging to place their malicious VM on the same physical machine as that of a target customer.

- extract confidential information via a cross-VM attack.

- While there are a number of avenues for such an attack, the paper focuses on side-channels: cross-VM information leakage due to the sharing of physical resources (e.g., the CPU's data caches).

THREAT MODEL

- Two kinds of attackers
  - those who cast a wide net and are interested in being able to attack some known hosted service
  - those who focused on attacking a particular victim service.
- The later task is more expensive and time-consuming than the former's, but both rely on the same fundamental attack.

Questions

- Can one determine where in the cloud infrastructure an instance is located?
- Can one easily determine if two instances are co resident on the same physical machine?
- Can an adversary launch instances that will be co-resident with other user's instances?
- Can an adversary exploit cross-VM information leakage once co-resident?

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