Cloud Security

Can one determine where in the cloud infrastructure an instance is located?

- **hypothesis**
  - Different availability zones are likely to correspond to different internal IP address ranges and the same may be true for instance types as well.
  - Mapping the use of the EC2 internal address space allows an adversary to determine which IP addresses correspond to which creation parameters.

- They evaluate the theory using two data sets:
  - One created by enumerating public EC2-based web servers using external probes and translating responsive public IPs to internal Ips (via DNS queries within the cloud)
  - Another created by launching a number of EC2 instances of varying types and surveying the resulting IP address assigned

Surveying public servers on EC2

- WHOIS queries
  - Identified four distinct IP address prefixes
- For the remaining IP addresses - performed a TCP connect probe on port 80.
- Via an appropriate DNS lookup from within EC2, we translated each public IP address that responded to either the port 80 or port 443 scan into an internal EC2 address.

Can one easily determine if two instances are co-resident on the same physical machine?

Network-based co-residence checks

- co-resident if they have
  - matching Dom0 IP address,
  - small packet round-trip times, or
  - numerically close internal IP addresses

Veracity of the co-residence checks

- Ability to send messages over a cross-VM covert channel
- If two instances can successfully transmit via the covert channel then they are co-resident, otherwise not

Can an adversary launch instances that will be co-resident with other user's instances?

observations

- A single account was never seen to have two instances simultaneously running on the same physical machine
- running n instances in parallel under a single account results in placement on n separate machines.
- No more than eight m1.small instances were ever observed to be simultaneously co-resident.
- While a machine is full an attacker has no chance of being assigned to it.

Brute-forcing placement

- Start by assessing an obvious attack strategy: run numerous instances over a (relatively) long period of time and see how many targets one can achieve co-residence with.

Can an adversary exploit cross-VM information leakage once co-resident?

- On stealing cryptographic keys
  - extracting cryptographic secrets via cache-based side channels.
- denial of service
- Measuring cache usage
  - Load measurement
- Load-based co-residence detection
- Keystroke timing attack

CONCLUSIONS

- 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