Exploring Information Leakage In Third-Party Compute Clouds

Summary : This paper shows the various vulnerabilities introduced in the cloud computing due to the virtualization of the resources by the provider. The use of virtualization allows the cloud providers to recover the huge capital invested in the cloud and thus maximize their gains. The papers talks about the novel abilities given to the attacker by the third-party cloud provider. Here Amazon's EC2 service is used to show that one can determine where in the cloud infrastructure a target VM is located and then launch a malicious VM that will be co-resident with the target VM. Once co-resident, an adversary can extract confidential information like CPU data caches, network queues , etc. This type of attack can be seen as a four step process. First the cloud cartography technique is used to map the EC2 service to understand where potential targets are located in the cloud. Instance type and available time zones are inferred based on the differences in the IP addresses. The second step is to determine co-residency. Instances co-residency is checked by matching Dom0 IP address, small packet round trip times, or numerically close internal IP addresses(e.g. within 7) . The third step is exploiting placement in EC2. Here the feasibility of achieving co-residency with the target VM is accessed based on the data gathered in the prior steps. Two techniques are discussed namely brute forcing placement and instance flooding. The last step is the cross VM information leak. Here a malicious instance utilizes side channels to learn information about co-resident instance. Prime + Probe technique is utilized to measure the cache activities like current load of the machine. A high load indicates activity on co-resident instance. Further detection of web traffic and key strokes of the victim can also be measured.

Opinion : The paper describes a well designed threat model which helps in analyzing security model, design strategies and evaluate solutions. The threat model consists of a trusted cloud provider, an attacker, who is a malicious cloud user and a victim, who is other cloud user with some sensitive information. The fundamental risk as per the paper arises from sharing physical infrastructure between users. The resolution given is to let user choose their VM placement and let them pay for their choices. Well in this case the user is burdened with the responsibility of placing the VM. This can be improved by the cloud provider by taking measures to encapsulate the physical design of the cloud with a logical design .

Pros and Cons : The paper is clearly based on multiple assumptions. To start with, it is assumed that internal IP addresses are static and that Dom0 will respond to the trace routes. Secondly, it is assumed that the attacker can launch many instances without even considering the cost associated with it. Lastly, if a machine is full then it cannot be attacked. This point also gives us insight to the fact that in order to maximize the gains, a cloud provider will start a new instance only when all the running instances are full. This will fairly increase the number of machines which are full. Now for the pros, this paper points out the threats associated with the side channel attacks in VMs. The attack model is well defined which uses simple tools. The mapping of the cloud fairly exposes the infrastructure of the EC2 service. Various measures are discussed which can prevent these types of attacks.