Deniz Aytemiz

Spectre Attacks: Exploiting Speculative Execution

Side-channel attacks leverage the hardware vulnerabilities to leak confidential information. In this paper spectre attacks are introduced and analyzed. Spectre attacks arise from inducing anomalous operations in the victim's machine to enable side channel attack. This paper shows how this methodology can be combined with side channel, fault attacks and return oriented programming to create practical attacking schemes. It also introduces practical methods for determining such attacks. The countermeasures described are only short term since long term countermeasures require fundamentally changing instruction set architectures due to the need of common understanding between hardware and software developers for CPUimplementation permission. Security can be increased however there will be performance trade-offs.

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

In this paper side channel attacks scenarios for co-resident Virtual Machines are discussed in terms of security of cloud computing Amazon EC2. Co-resident VMs are vulnerable considering side-channel attacks since they use the same physical architecture. Authors describe how they make queries for obtaining internal IPs of EC2 servers and map the EC2 instances' internal IP addresses to availability zones and instance types. The map is later used by the adversary to increase the possibility of achieving co-residency with a malicious VM. Then the checks for achieving co-residency and the network probes required are discussed. Two methods; brute forcing and abusing placement locality for achieving co-residency are discussed. Placement locality method leverages the tendency of EC2 assigning roughly same time running instances parallely to the same physical machine. Finally all the methods and methodologies discussed are used to achieve a side-channel attack. The countermeasures for security as not allowing non-trusted parties co-residency is introduced.