Security is essential for the success of the infrastructure-as-a-service (IaaS) business model, a key component of the popular "cloud" concept. Mission-critical virtual machines (VMs) running in clouds handle sensitive information that must be protected and run applications whose operation must not be compromised. These VMs often need to exchange information with peers outside the cloud in order to fulfill their tasks.

To improve efficiency and cut costs, popular IaaS providers offer users a virtualized environment running on top of shared hardware. This is a sensible strategy in many respects, but it opens up the possibility of side-channel attacks. Moreover, exchanging data across the cloud boundaries requires the VMs to be reachable from the Internet. However, the traditional way of accomplishing this by using public IP addresses makes the VMs vulnerable to denial-of-service (DoS) attacks.

My role in the project was to design and implement an algorithm intended to decrease the likelihood of a successful side-channel attack. This algorithm:

- automatically schedules and manages migrations to random hosts and at random times within user-defined time ranges.
- coordinates the migrations with a tailored peer-to-peer virtual private network controller in order to reduce the reconnection latency after each migration.

The design and implementation of an algorithm to diminish the likelihood of a successful side-channel attack by automatically scheduling and managing migrations to random hosts and at random times within user-defined time ranges. It reduces the VMs' vulnerability to DoS attacks by effectively limiting the attack vectors to the IaaS environment and transparent to the applications running on the VMs. It reduces the VMs' vulnerability to DoS attacks by effectively limiting the attack vectors to the IaaS internal network.

The system presented in this poster is based upon the work supported by Diana Machado. I am thankful for the help that I received from my teammate Raul Garcia and my mentor Dr. Ming Zhao.