Self-Stabilizing Cloud Infrastructure

Researchers

Prof. Shlomi Dolev
dolev@cs.bgu.ac.il

Dr. Alexander Binun
binun@cs.bgu.ac.il

Dr. Reuven Yagel
yagel@cs.bgu.ac.il

Tomer Godinger
tomergod@post.bgu.ac.il

Mark Bloch
markbl@post.bgu.ac.il

Boaz Menuhin
boaz.menuhin@gmail.com

Martin Kahil
kahil@post.bgu.ac.il

Goals

The main goal is to obtain a robust self-stabilizing cloud. Such a cloud will need far less human intervention to function and will be capable of fast recovery from various attacks.

The intermediate goal is to build a self-stabilizing local hypervisor that ensures smooth and correct execution of each Virtual Machine (VM) and protects it from negative effects posed by malware attacks and possible Byzantine behavior of VMs in a system.

Eventually we aim to extend the self-stabilizing local hypervisor to the distributed cloud. We intend to achieve this goal using the open-source distributed cloud provider OpenStack.

Description

Our self-stabilizing hypervisor demonstrates robustness in the presence of transient faults in VMs and Byzantine VMs. The cloud is becoming more and more popular, thus the need for resource utilization. All cloud providers exploit virtualization to achieve optimal utilization of resources, and to provide privacy to each client. Nonetheless, security remains a major issue, since VMs may break out of the virtual environment and take over the actual host. Rigid security policies may decrease system performance and/or restrict collaborations, thus potentially affecting service level agreements (SLAs). An automatically recovering system of virtual machines helps provide security, while still meeting SLAs, making a great contribution to the field.

We have developed a self-stabilizing architecture, augmenting the widely known KVM hypervisor with self-stabilization facilities. A system comprising several VMs is able to recover after transient failures and attacks (e.g. denial of service, worms, corruption of sensitive memory areas).

We are currently extending the prototype into the distributed world. We are deploying and running attack scenarios on OpenStack, simulating the comprehensive attack model and the approach to recover a distributed cloud. We note that, during the first research phase, the defenses against certain threats were hardcoded into our module. During the following phase, we support generic user-defined defense specifications.

This research could save a lot of money and human interaction while managing a cloud. In addition, the automatic recovery from transient faults and attacks will make it more feasible to meet certain SLAs.