Computer Systems Lab

Project Proposal in Concurrent and Distributed Systems 236371

Winter 2014

Resource Tradeoff for Cryptanalytic Algorithms in a Resource-as-a-Service (RaaS) cloud

Description:

Current trends in the Infrastructre-as-a-Service (IaaS) clouds are likely to result in a new cloud model: the Resource-as-a-Service (RaaS) cloud[1]. In the RaaS cloud resources such as bandwidth, CPU and RAM may change hands every second, on the basis of economic considerations. Thus, the price of different resources may change with time, in response to changes in demand.

In this project the student will build a RaaS application that changes its consumption of different resources in response to their changing prices. The student will combine existing cryptanalytic techniques (attacks on cryptographic primitives) according to varying pricing data.

Prerequisites:

Operating systems course (or equivalent knowledge).

[Advantage: Modern Cryptology or Computer Security courses]

Platform:

A Linux virtual machine under KVM.

Advisors: Assaf Schuster, Orna Agmon Ben-Yehuda, Orr Dunkelman

{assaf,ladypine,orrd} at cs.technon.ac.il

Number of students: 1 or 2 students.

References:

[1] ”The Resource-as-a-Service (RaaS) cloud”, Orna Agmon Ben-Yehuda, Muli Ben-Yehuda, Assaf Schuster, Dan Tsafrir. In proceedings of the 4th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud) 2012.