SES CHARLES V. SCHAEFER, JR. SCHOOL OF ENGINEERING AND SCIENCE

STEVENS INSTITUTE of TECHNOLOGY THE INNOVATION UNIVERSITY

MATHEMATICAL SCIENCES Colloquium

Logic, Policy, and Federation in the Cloud

Yuri Gurevich

Microsoft Research

Monday, March 21, 2011
4:00-5:00pm
Babbio 104

Abstract

Imagine that you manage a public cloud. You want to attract lucrative customers but they worry that their data might not be secure in your cloud. Of course they can encode their data before putting it in and decode it upon removal but that doesn't buy much for them (or for you because your cloud is used just as a glorified blob store). How can you add value? Cryptographers have many tricks but few of them are feasible at this point. But maybe we shouldn't reinvent the wheel. How do enterprises interact in real world? Consider commerce for example. Buyers and sellers from countries different in geography, culture and political system succeed in making mutually beneficial deals. The sellers get paid, and the buyers get their goods. How does it work? Well, there is an involved support system developed from centuries of experience: banks issuing letters of credit, insurance companies underwriting the transactions and transportation, etc. And numerous policies are enforced. Similarly, there is an involved support system that allows Big Pharma to conduct clinical trials that straddle multiple countries. And so on. Can we lift such support systems to the cloud scale and make them more efficient in the process?

An important ingredient of the desired solution is a high-level policy language. As we mentioned above, numerous policies need to be enforced. They also need to be stated formally to allow automation, and they need to be high-level to allow comprehension and reasoning. Cryptography is indispensible in enforcing policies but first we need a language to formulate policies succinctly and to exchange them among autonomous parties. The Distributed Knowledge Authorization Language (DKAL) was created for such purposes. It required foundational logic investigation, and it is in the process of tech transfer. This lecture is a popular introduction to DKAL and its applications to doing business via public clouds.

Bio:
Yuri Gurevich is Principal Researcher at Microsoft Research in Redmond, WA. He is also Prof. Emeritus at the University of Michigan, ACM Fellow, Guggenheim Fellow, a member of Academia Europaea, and Dr. Honoris Causa of a Belgian and Russian universities.

Refreshments served at 3:45pm.