Karlsruher Institut für Technologie

KOLLOQUIUM

Informatik-Sonderkolloquium

Logic, Policy, and Federation in the Cloud

Yuri Gurevich, Research in Software Engineering

Imagine that you manage a public cloud. You want to attract lucrative customers but they worry that their data will not be secure in your cloud. Of course they can encode their data before putting it in the cloud 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; most notably, searching on encrypted data with a single keyword is being considered. But maybe we shouldn't reinvent the wheel. How do enterprises interact in real world? Consider commerce for example. Buyers and sellers from very different (in geography, culture, political system) countries 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 that developed from centuries of experience: banks issuing letters of credit, insurance companies that underwrite 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?

We believe that the answer is YES. An important ingredient of the desired solution is a high-level language for writing policies. 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.

KIT – Campus Süd, Fakultät für Informatik, Am Fasanengarten 5, 76131 Karlsruhe, www.informatik.kit.edu

Freitag, 26.11.2010, 15:30 Uhr

Informatik-Hauptgebäude (50.34), SR 301 3.OG), Am Fasanengarten 5, 76131 Karlsruhe