Logical Methods for Data Security

Mikheil Rukhaia

Institute of Applied Mathematics, Tbilisi State University.
mrukhaia@logic.at

The talk is divided into two parts and mainly consists from preliminary work of two different projects.

First part is about rule-based approach to attribute based access control. Formal description of access control is extremely important, since it should be defined, unambiguously, how rules regulate what action can be performed by an entity on the resource, how to guarantee that each request gets an authorization decision, how to ensure consistency, etc. We aim at specifying ABAC operational and administrative models in a formalism, which combines the power of conditional rewriting and logic programming, based on the ρLog calculus.

In the second part, we consider problem of cryptographic protocol verification and analysis. Cryptographic protocol is used for secure communication over the network by two or more agents. Cryptographic protocol verification is a task, that determines whether the protocol is secure and can be broken by different kind of attacks, like "men in the middle", etc. We try to model a cryptographic protocol in the Pρlog system and show whether it is vulnerable for attacks. We would like to mention, that it is easier task (decidable) to find out whether a protocol is vulnerable for attacks, than to find an attack that breaks the protocol (not decidable in general).