ლოგიკური მეთოდები მონაცემთა უსაფრთხოებაში

მიხეილ რუხაია

გამოყენებითი მათემატიკის ინსტიტუტი, თბილისის სახელმწიფო უნივერსიტეტი.
mrukhaia@logic.at

მოხსენება გაყოფილია ორ ნაწილად და შედგება ორი დამოუკიდებელი პროექტის წინარე სამუშაოსგან.

პირველი ნაწილი ეხება წესებზე დაფუძნებულ მიდგომას ატრიბუტებზე დაფუძნებული წვდომის კონტროლის მიმართ. წვდომის კონტროლის ფორმალური აღწერა უაღრესად მნიშვნელოვანია, რადგან ცალსახად უნდა განისაზღვროს, თუ როგორ არეგულირებენ წესები სუბიექტის რესურსზე მოქმედებას, როგორ უნდა იქნას უზრუნველყოფილი ის, რომ თითოეულ მოთხოვნას ავტორიზაციის გადაწყვეტილება მოსდევდეს, როგორ უნდა იქნას გარანტირებული არაწინააღმდეგობრიობა და სხვ. ჩვენი მიზანია ABAC-ის ოპერაციული და ადმინისტრაციული მოდელების ისეთ ფორმალიზმში განსაზღვრა, რომელიც პირობებიან გადაწერას და ლოგიკურ პროგრამირებას აერთიანებს, ρLog აღრიცხვის საფუძველზე.

მეორე ნაწილში განვიხილავთ კრიპტოგრაფიული პროტოკოლების შემოწმებისა და ანალიზის ამოცანას. კრიპტოგრაფიული პროტოკოლები გამოიყენება ქსელში ორ ან მეტ აგენტს შორის უსაფრთხო კომუნიკაციისათვის. კრიპტოგრაფიული პროტოკოლების შემოწმება არის ამოცანა, რომელიც ადგენს თუ რამდენად დაცულია პროტოკოლი და შესაძლოა თუ არა მისი გატეხვა სხვადასხვა შეტევებით, მაგალითად, "men in the middle", და სხვ. ჩვენი მიზანია კრიპტოგრაფიული პროტოკოლის მოდელირება Pρlog სისტემაში და იმის ჩვენება, თუ რამდენად დაცულია ის. აქვე გვინდა ავღნიშნოთ, რომ პროტოკოლის დაცულობის შემოწმება უფრო ადვილი ამოცანაა (ამოხსნადი), ვიდრე ის, რომ ვიპოვოთ შეტევა, რომელიც ტეხავს პროტოკოლს (საზოგადოდ ეს ამოცანა ამოხსნადი არ არის).