Faculdade de Ciências da Universidade de Lisboa
cmafcio@fc.ul.pt Tel. (+351) 21 750 00 27

SEMINÁRIO DE LÓGICA MATEMÁTICA

Dia 10 de Setembro (segunda-feira), sala 6.2.38 às 16:00

A labeled logic for analyzing cyber-forensics evidence

Luca Viganò
(King´s College London)

Abstract:

The frequency and harmfulness of cyber-attacks are increasing every day, and with them also the amount of data that the cyber-forensics analysts need to collect and analyze. We propose a formal analysis process that allows an analyst to filter the enormous amount of evidence collected and either identify crucial information about the attack (e.g., when it occurred, its culprit, its target) or, at the very least, perform a pre-analysis to reduce the complexity of the problem in order to then draw conclusions more swiftly and efficiently.
We introduce the Evidence Logic EL, a labeled logic for representing simple and derived pieces of evidence from different sources. We propose a procedure, based on monotonic reasoning, that rewrites the pieces of evidence with the use of tableau rules, based on relations of trust between sources and the reasoning behind the derived evidence, and yields a consistent set of pieces of evidence.

Seminário financiado por Fundos Nacionais através da FCT – Fundação para a Ciência e a Tecnologia no âmbito do projeto UID/MAT/04561/2013

Local: FCUL, C6 - Piso 2, 6.2.38