Guest Lecture

HAEC

Complexity of Anonymity for Security Protocols

Prof. Ferucio Laurentiu Tiplea

Department of Computer Science
“Alexandru Ioan Cuza” University of Iasi
Iasi, Romania

Monday, 10.04.2017, 13:00 – 14:00, TU Dresden, Fakultät Informatik
Nöthnitzer Str. 46, Raum APB-1004

Abstract:
Anonymity, as an instance of information hiding, is one of the security properties intensively studied nowadays due to its applications to various fields such as e-voting, e-commerce, e-mail, e -cash, and so on.

In this talk we discuss the decidability and complexity status of the anonymity property in security protocols. We show that anonymity is undecidable for unrestricted security protocols, is NEXPTIME-complete for bounded security protocols, and it is NP-complete for 1-session bounded security protocols. In order to reach these objectives, an epistemic language and logic to reason about anonymity properties for security protocols under an active intruder, are provided. Agent states are endowed with facts derived from actions performed by agents in protocol executions, and an inference system is provided. To define anonymity, an observational equivalence is used, which is shown to be decidable in deterministic polynomial time.

Bio:

Ferucio Laurentiu Tiplea received the Ph.D. degree in computer science from ``Alexandru Iona Cuza'' University of Iasi, Romania, in 1993. He joined the Department of Computer Science of the aforementioned university in 1990, where he is currently Professor of Computer Science.

Dr. Tiplea's research interests lie in the area of theories and tools for high-level modeling, design, and analysis of systems (including Petri nets and formal verification), complexity of computation, and cryptography and computer security. He published more than 80 papers in professional journals and refereed conference proceedings in these areas, co-edited five conference volumes, contributed to six edited volumes, and delivered invited talks at many universities and international conferences. Dr. Tiplea was the recipient of several fellowships, such as the Fulbright Fellowship, German Academy Fellowship, DAAD Fellowship, Monbusho Fellowship. From December 2003 to May 2006 he held a Visiting Professor position at University of Central Florida, School of Computer Science, Orlando (USA).

TECHNISCHE UNIVERSITÄT DRESDEN

DRESDEN concept

DFG