

Call for Applications

Course on "Security: From Basic Concepts and Techniques to Formal Models and Methods"

Iași, Romania, 4–8 April, 2006

Course Description

Security has become more and more significant in information technology, especially in those applications involving data sharing, communication and transactions through the Internet. In addition, security policies and standards are starting to be enforced by a growing number of legislative mandates.

This course will introduce basic concepts used in security, such as confidentiality, integrity and availability, and examine basic techniques necessary to implement security, such as cryptography, key management and security protocols.

Various formalisms based on interaction among processes are presented as general frameworks for describing security protocols. They include the process algebra CCS, the pi-calculus, and variants of the pi-calculus. We take as a case study the Needham-Schroeder protocol; we express this protocol in Spi calculus which is an extension of the pi-calculus with primitives for encryption and decryption, and we prove its authentication and secrecy. Participants could be involved in small projects where they will apply certain formal models and methods to solve some security problems.

Lecturers

Dr. Antonio Cerone (*United Nations University, Macau SAR China*) is a Research Fellow of UNU-IIST, the United Nations University International Institute for Software Technology. He is the Chair of the Steering Committee of the International Conferences on Software Engineering and Formal Methods and the Regional Representative for South-East Asia of the European Association of Software Science and Technology (EASST). He holds a PhD and an MSc in Computer Sciences from the University of Pisa, Italy. His research interests include formal specification and verification, concurrent and real-time systems, security and human-computer interaction.

Dr. Gabriel Ciobanu is a researcher working at the Institute of Computer Science, Romanian Academy (Iasi Branch). He is also affiliated to the "A.I.Cuza" University, Faculty of Computer Science. His research interests include Distributed Systems and Concurrency, Theory of Programming, and Computational Models and Methods in Biology. He has edited/authored 5 books and many papers on these topics. For his research in these areas, he received the 2004 Octav Mayer Award and the 2000 Grigore Moisil Award of the Romanian Academy of Sciences. He was a visiting academic to Edinburgh University, Paris XI, Tohoku University, and National University of Singapore, among others.

Requirements

The course is devoted to Master and PhD students, as well as postgraduate students and researchers from academia and industry who

- are citizens of a developing country not belonging to the European Union;
- do not hold any position in an industrialised country or in a country belonging to the European Union;
- have obtained at least an undergraduate degree in Computer Science or in a related discipline;

where **developing countries** are those countries whose economies are classified as *low, lower-middle and upper-middle income*, and **industrialised countries** are those countries whose economies are classified as *high income* by the World Bank at <http://www.worldbank.org/data/countryclass/classgroup.htm>.

Application and Deadline

An Application must include:

- completed Application Form (available for download at <http://www.iist.unu.edu/~antonio/Training/2006-04-SPTV-iasi-romania.html>);
- scanned copy of the university transcript for the completed undergraduate degree;
- any further qualification and information that should be taken into account, e.g. a list of publications.

Applications should be sent by email to

gabriel@iit.tuiasi.ro and antonio@iist.unu.edu

no later than Monday 20 March 2006.

All documents must be attached to the email (possibly scanned).

Financial Support

Applicants who need financial support must explicitly request it in the Application Form. UNI-IIST will provide financial support to a limited number of applicants who have requested it and are affiliated to institutions located in places from which it is not possible to travel on a daily basis to the course venue. The financial support consists of

- the reimbursement of the travel expenses for a return trip from the location of the participant's institution to the course venue, and
- accommodation for 4 consecutive nights in Iași, starting on Monday 3 April.

Participants will be reimbursed in US dollars, according to the UN official exchange rate, upon presentation of original receipts (which will be kept by UNU-IIST) up to a maximum amount decided by UNU-IIST. Travel expenses will only be reimbursed for the cheapest transportation along the most direct route. Only 2nd class tickets will be reimbursed for train trips and only economy class fares will be reimbursed for air trips. Airfares will not be reimbursed to participants from Romania. No reimbursements will be given for meals, local transportation, taxi, fuel and road toll. All UNU-IIST decisions regarding reimbursements are final.

Venue, Schedule, Fee and Certificate

The course will be held at the Faculty of Computer Science, "A.I.Cuza" University, from Tuesday 4 to Saturday 8 April. Each day will start at 9am and terminate approximately at 6pm, with a 2 hour break during the lunch time. Saturday will be mainly devoted to discuss the project topics.

There is no fee for participating in the course.

Every participant will receive an attendance certificate issued by the United Nations University.

Local Organising Institution

The Local Organising Institution, "Alexandru Ioan Cuza" University, Faculty of Computer Science, is the oldest Romanian (modern) university, and was ranked 1st in Romania for 2004 (based on the ISI publications).