



Università degli Studi di Verona

Scuola di Dottorato di Scienze Ingegneria e Medicina

Ca' Vignal 2
Strada le Grazie 15
37134 Verona - Italia
Tel. +39 045 802 7069
Fax +39 045 802 7068

Dipartimento di Informatica

**Information Security:
From an Art to a Science**

Lectio Magistralis

September 13, 2007

David Basin

ETH Zurich
Switzerland

Abstract - Information security is central to the proper functioning and acceptance of a wide spectrum of modern systems. Unfortunately, constructing secure systems is difficult as developing secure building blocks "in the small" and their composition to systems "in the large" are both error-prone activities. In this talk, I will show how formal methods --- in particular the use of formal models combined with symbolic computation --- can be employed to tackle both kinds of problems. As examples, I present results on analyzing security protocols, and the automatic generation of secure software-architectures for middleware-based distributed systems from high-level models.

The lecture will take place at **4:00 pm** in the **Sala Verde** of the
Dipartimento di Informatica - Ca' Vignal 2, Strada le Grazie 15, 37134 Verona, Italy

Local organization and contact: Prof. Luca Viganò
luca.vigano@univr.it

Web info: www.di.univr.it

Note on the Lecturer - Prof. Dr. David Basin (<http://www.inf.ethz.ch/~basin>) is a full professor and has the chair for Information Security at the Department of Computer Science of ETH Zurich, Switzerland, since January 2003. He is also the director of the Zurich Information Security Center ZISC, a co-operation between members of ETH Zurich and industry, with the aim of providing a coordinated program of state-of-the-art research and education in information security. He received his Ph.D. from Cornell University in 1989, and his Habilitation from the University of Saarbrücken in 1996. He held a postdoctoral research position at the University of Edinburgh (1990-1991), he led a subgroup, within the programming logics research group, at the Max-Planck-Institut für Informatik in Saarbrücken (1992--1997), and he held a full professor chair in software engineering at the University of Freiburg (1997--2002). His research focuses on information security, in particular methods and tools for modeling, building, and validating secure, reliable systems. He has co-authored over 100 publications. He has taught numerous courses, tutorials, and industrial courses on information security, at universities and international schools, and he has organized, or been a member of, the program committee of over 80 international conferences and workshops. He is an editor of 4 international journals. He has participated in and/or co-ordinated a number of projects at the national and international level on trust and security.