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

**Dottorato di ricerca in Informatica**

**Graduate course in**

# Introduction to Engineering and Formal Methods for Information Security

**September 11-18, 2007 (16 hours)**

Prof. Dr. David Basin

Department of Computer Science
ETH Zurich
Switzerland

## Description

We will examine different methods for developing and validating secure systems. This includes methods for developing security infrastructures for large-scale distributed systems, as well as methods for verifying the security of subsystems and security infrastructure, such as security protocols.

We begin with the topic of **Security Engineering**, which is an evolving discipline that unifies two important areas: software engineering and security. We present an approach to integrating security into the system design process. Namely, models are made of system designs along with their security requirements, and security architectures are automatically generated from the resulting security-design models. We call the resulting approach "Model Driven Security" as it represents a specialization of model driven development to the domain of system security. We describe this approach in detail, present the UML-based modeling language SecureUML, describe its theoretical foundations, and show it can be used in practice.

The second area we consider is the use of **Formal Methods** to verify the building blocks used for constructing secure systems. Here we provide an introduction to automated methods and tools for formally specifying and analyzing security protocols. First, we introduce security protocols, some of the difficulties in reasoning about them, and briefly survey the different kinds of formal methods available to tackle this problem. In the second part, we present OFMC, the On-the-Fly Model Checker developed at ETH Zurich and the AVISPA tool, a state-of-the-art tool for analyzing security protocols. We explain the theory behind these tools and show how they can be used to reason about complex Internet protocols, like those under development by standardization bodies like the IETF.

The course will include laboratory exercises.

## CONTENTS

### Week 1 – September 11/14, 2007

**11/09 (14.30-16.30) – Model Driven Security, part 1 (2 hrs)**

1.1 Course introduction
1.2 Modeling secure components
1.3 Semantics

**12/09 (14.30-16.30) – Model Driven Security, part 2 (2 hrs)**

2.1 Generating security infrastructures
2.2 Secure controllers
2.3 Experience with Model Driven Security in practice

**13/09 (16.00-17.30) - Information Security: From an Art to a Science (1.5 hrs)**

3. General lecture on the role of formal methods for information security

**14/09 (10:30-12:30 and 14.30-16.30) - Model Checking Security Protocols using OFMC (4 hrs)**

4.1 Introduction to security protocols
4.2 Formal protocol analysis
4.3 OFMC
4.4 Conclusions

### Week 2 – September 17/18, 2007

**17/09 (16.00-17.30) – Security Automata (1.5 hrs)**

5.1 Execution monitoring
5.2 Security Automata
5.3 Specifying Security Automata using CSP-OZ
5.4 Examples
5.5 Conclusions

**18/09 (09.30-12.30 and 14.30-16.30) - Security Protocol Verification Laboratory using OFMC (5 hrs)**

6. Lab work using the OFMC model checker.

Lectures will take place at the
**Sala Verde**
**Dipartimento di Informatica**
**Ca' Vignal 2 - Strada le Grazie 15, 37134 Verona, Italy**

The course is supported by the Università degli Studi di Verona, with a CooperInt grant and by the Dipartimento di Informatica.

The admission to the course is FREE. Attendees must submit an application via email to the local organizer indicating their affiliation and current position by **September 7, 2007**.

Proficiency certificates or equivalent credits will be provided on request and upon completion of independent homework.

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

Web info: `www.di.univr.it`