Available online at www.sciencedirect.com

SCIENCE DIRECT®

Electronic Notes in Theoretical Computer Science

ELSEVIER

Electronic Notes in Theoretical Computer Science 99 (2004) 1–2

www.elsevier.com/locate/entcs

Preface

The project MEFISTO (*MEtodi FormalI per la Sicurezza e i TempO*, i.e., formal methods for security and time) was a italian national project funded by the Ministry of Education, University and Research. It lasted two years, from Dec 2001 to Dec 2003, with an overall funding of about 300,000 euros. The sites forming the consortium were: University of Bologna (Roberto Gorrieri, national coordinator of the project), University of Pisa (Pierpaolo Degano, local coordinator), University of Salerno (Margherita Napoli), University of Trento (Corrado Priami), University of Venice (Riccardo Focardi).

The project aimed at studying the theoretical foundations for the analysis and design of secure communication protocols for distributed systems. The background goal was a detailed study of the definitions of the basic properties of interest (such as, e.g., confidentiality, authentication, integrity, non repudiation, noninterference, etc..). The intention of this study was to provide a thorough and formal classification of the various definitions found in the literature, so as to enable an evaluation of their relative merits. The project was organized into three main themes:

(i) Static analysis techniques

(ii) Behavioural (or dynamic) techniques

(iii) Fine grain models

The first two themes studied security properties for coarse grain models such as classic nondeterministic automata (or labeled transition systems) and process algebras that take semantics on them (e.g., CCS, CSP, spi-calculus, CryptoSPA). Theme (*i*) is devoted to static analysis techniques (such as types, control flow and abstract interpretation), while Theme (*ii*) to dynamic or behavioural techniques (such as equivalence checking and model checking) to verify the correctness of the various security properties. Theme (*iii*) is instead concerned with the less studied problem of security in the setting of fine

1571-0661
doi:10.1016/j.entcs.2004.06.001

grain models, i.e. models where more concrete information on the behaviour of systems (e.g., time and probability) is represented. There is a large variety of timed/probabilistic/stochastic models and languages that are useful to model systems working under real-time constraints or quality of service requirements; this theme will study the security issues of such systems, where it is often crucial to study the trade-off between the degree of security guarantees and the degree of the offered quality of service.

This ENTCS volume collects some papers from the partners of the project and can be seen as reasonable panorama of the research themes that have been addressed during the two-year project. The topics of the papers range from information flow security (also in their probabilistic variant) to authentication protocols, from secure program transformation to analysis of imperfect cryptography, with case studies in electronic commerce and certified mail protocol. The 15 selected contributions have undergone a severe refereeing procedure.

Mario Bravetti
Roberto Gorrieri
March 2004