Università
Ca'Foscari
Venezia

PROJECT ACRONYM AND TITLE: **Formal Specification for Secured Software System**

FUNDING PROGRAMME: **MAECI Italia - India**

CALL: **Bando MAECI Italia - India**

SCIENTIFIC FIELDS: **Technologies applied to Cultural and Natural Heritage**

HOST DEPARTMENT: **Department of Environmental Sciences, Informatics and Statistics**

SCIENTIFIC RESPONSIBLE: **Agostino Cortesi**

ABSTRACT:

The traditional paradigm for deploying a secure software system almost always results in designing the system first, and considering security as an afterthought. This in turn creates monumental problems when such systems become operational. In fact, in mainstream software engineering methodologies, security and privacy constraints are often just declared in the list of non-functional requirements (to be checked only at deployment time), hence, lacking (1) a proper formalization, and (2) a clear traceability with respect to the related functional requirements.

The objective of the project is to investigate whether security policies of a (possibly safety critical) system could be integrated into the formal requirement specification using formal methods, in order to detect ambiguities and inconsistencies within the specification phase in Software development life-cycle. In this direction, we will apply lightweight techniques for validation and verification towards securing the application right at the requirement engineering stage. In particular, we will apply modeling languages like Event-B and iSTAR to specify and analyze the requirements so that the design of application software itself is compliant to the security criteria. All in all, the proposed research work caters for the increasing need of mathematically well-founded techniques to validate security aspects of application software.

Planned Start date	Planned End date
18th April 2017	31st December 2019

PARTNERSHIP:

1	Università Ca' Foscari Venezia	Italy	Coordinator
2	University of Calcutta	India	Partner