IRM PRESS

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.irm-press.com

ITB9162

Chapter IV

A Methodology for Developing Trusted Information Systems: The Security Requirements Analysis Phase

Maria Grazia Fugini
Politecnico di Milano, Italy

Pierluigi Plebani
Politecnico di Milano, Italy

ABSTRACT

In building cooperative distributed information systems, a methodology for analysis, design and implementation of security requirements of involved data and processes is essential for obtaining mutual trust between cooperating organizations. Moreover, when the information system is built as a cooperative set of e-services, security is related to the type of data, to the sensitivity context of the cooperative processes and to the security characteristics of the communication paradigms. This paper presents a methodology to build a trusted cooperative environment, where data sensitivity parameters and security requirements of processes are taken into account. The phases are illustrated *and a reference example is presented in a cooperative information system and e-applications. An architecture for trusted exchange of data in cooperative information system is proposed. The requirements analysis phase is presented in detail.*

INTRODUCTION

Recently, the widespread use of information technology and the availability of networking services have enabled new types of applications in the field of Information Systems, characterized by several geographically distributed interacting organizations exchanging data through the network and the Web. For example, *Cooperative Information Systems* (*CoopIS*) are distributed information systems that are employed by users of different organizations under a common goal (Mylopoulos et al., 1997). Another extension consists of *e-applications* (Mecella et al., 2001), namely, *e-services* provided by different organizations on the net. The data exchange and the interleaved execution of processes in such systems bring about security issues bound to inter- and intra-organizational structures, to a plurality of actors in the distributed system, and in the heterogeneity of policies existing at the various sites where a distributed process is executed.

In advanced information systems, new security issues, besides traditional ones, arise, such as (1) cooperating organizations may not know each other in advance; (2) data exchanged in a cooperative environment can be either internally generated or acquired from other sources. Newly created data can have different security levels according to their acquisition mode (e.g., manual data entry vs. automatic capture) and their information acquisition process; (3) e-applications can be invoked in a distributed way at design and at run-time and, whereas in traditional "closed" CoopIS mutual knowledge and agreements upon design of applications are the basis for the cooperation, the availability of a complex platform for CoopIS (Mecella et al., 2001) allows for "open" cooperation among different organizations that may not know and/or trust each other.

A major obstacle in securing new information systems lies in the lack of concepts and methods that, differently from traditional systems where security problems are well known [see for instance (Icove et al., 1995) for an overview], allow security developers to identify, design, and implement security requirements and policies that integrate different security needs in a heterogeneous system (Chung et al., 2000; Schneider, 2000).

For example, for CoopIS few requirements and policies are known at design time: at run time, policies need to be negotiated among the cooperating processes or new policies must be added. In these cases, determining the suitable requirements and policies is based on the identification of the "normal" behaviour of the system users (Mukkamala et al., 1999), known as user profiling methods. The need arises