

Framework and Methods for the Study and Analysis of Trust in Information Systems

Rubén Prieto-Díaz
Commonwealth Information Security Center
James Madison University
Harrisonburg, VA 22807
prietodiaz@cisat.jmu.edu

The goal of this minitrack is to generate research interest in the core concepts of trusted computing: fundamental issues about trust and how trust can be specified designed and programmed into information systems. There is an urgent need for an ability to specify and unambiguously define the characteristics that make computer systems trustworthy.

Five papers were accepted to this minitrack based on review recommendations from several reviewers for each paper. The papers form two groups. The first group reports on case studies dealing with trust management, requirements definition for trusted systems and architectural considerations for intrusion detection. The second group, which consists of the last two papers, focuses on solutions to specific research problems in trusted systems that have been eluding the research community for some time. The five papers are summarized below.

The paper by Brent Chun and Andy Bavier presents a layered architecture for dealing with three key trust management problems: how to express and verify trust, how to monitor trust, and how to manage and reevaluate trust relationships through time. These problems close the loop on trust management and are specially relevant in the context of federated systems. The authors argue that better facilities for decentralized trust management in federated systems would allow for a better way to verify, monitor and manage trust. They demonstrate their approach using the PlanetLab network testbed.

The paper by Jim Alves-Foss and Daniel Conte de Leon reports on an XML-based approach for implementing traceability among software work-products. The authors introduce an XML derivative requirements markup language for creating traceable

links between requirements, design and code for assessing the impact of requirements or design changes on other workproducts. The authors argue that ability to navigate from informal requirements to more formal requirements improve our ability to assess systems trustworthiness before systems are built.

The paper by Ambareen Siraj, Rayford Vaughn and Susan Bridges reports a research effort on a multi-sensor intrusion detection system as an aid for apprising system trustworthiness. They describe a Decision Engine for an Intelligent Intrusion Detection System (IIDS) that fuses information from different intrusion detection modules using fuzzy cognitive maps and fuzzy rule-bases. The paper presents the IIDS architecture and discusses preliminary experimental results on its use in the context of a Health Assessment Network.

The paper by Sam Redwine explores issues in Exclusion Basis Systems presented in a paper by Morales, et.al., at last years's HICSS version of this minitrack. The paper provides a method for dealing with multiple participants in a multicast system when leaving simultaneously. The problem of securely broadcasting new keys to the remaining participants is addressed as well as ways of encrypting messages for a subset of participants.

The paper by Mohamed Eltoweissy and collaborators explains how to apply an encryption and group key management scheme (presented in last year's HICSS version of this minitrack) in the domain of electronic service providers (ESPs) using trusted information distribution (TID) services as information brokers. The paper demonstrates the feasibility and effectiveness of the approach.