SECURE: Secure Environments for Collaboration among Ubiquitous Roaming Entities

Fact Sheet

Project Information

SECURE

Grant agreement ID: IST-2001-32486

Project website

Project closed

Start date
1 January 2002

End date
30 June 2005

Funded under
Programme for research, technological development and demonstration on a "User-friendly information society, 1998-2002"

Total cost
€ 1 729 860,00

EU contribution
€ 1 340 000,00

Coordinated by
THE PROVOST FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN
Ireland

This project is featured in...

Objective

It is arguable whether the security mechanisms used to protect today's information systems are adequate. What is clear is that new approaches to security are needed for the infrastructure envisaged by the global computing initiative, which is characterized by decentralised control. The SECURE project will investigate a new approach to security founded on the notion of trust. The project aims to develop a model in which trust relationships are established from the record of interaction between entities, and a security mechanism expressed in terms of such trust. SECURE will also investigate how to specify access control policy based on trust. The project will formally define a computational trust model and a collaboration model capturing the dynamic aspects of the trust model; means to specify and to enforce security policies based on trust; means to evaluate security policies and implementations based on trust; and algorithms for trust management.

OBJECTIVES
The objectives of SECURE are the definition of a computational trust model allowing entities to reason about the trustworthiness of other entities for use in security related decisions; the definition of a collaboration model capturing the issues of trust formation, trust evolution, trust propagation and trust exploitation; the definition of means to specify and to enforce security policies based on trust including specifying the level of positive experiences required to allow a particular principal access to a specific resource; the definition of means to evaluate security policies and implementations based on trust while recognizing that there may be many different ways of establishing the required level of trust for collaboration to take place; the development of a framework encompassing algorithms for trust management include algorithms to handle trust formation, trust evolution and trust propagation; the validation of the approach in the context of the formal model.

DESCRIPTION OF WORK
The application of trust leads naturally to a decentralised approach to security management that can tolerate partial information albeit one in which there is an

inherent element of risk for the trusting entity. Fundamentally, it is the ability to reason about trust that allows entities to accept risk when they are interacting with other entities and hence, the central problem to be addressed by SECURE is to provide entities with a basis for reasoning about trust. Thus, the heart of the SECURE workplan is the development of a computational model of trust that will provide the formal basis for reasoning about trust and for the deployment of verifiable security policies. The most important activity in the workplan is therefore the development of a formal computational trust model that captures human intuitions about trust, and must especially allow computational entities to reason about the trustworthiness of other participants for use in security related decisions. We have planned to deliver two revisions of the model during the course of the project primarily because we expect the development of the model to be informed by the other activities in the project.
While the development of the computational trust model is at the heart of SECURE, it alone is not sufficient to allow us to deliver a feasible security mechanism for the global computing infrastructure. In this context it is equally important that we understand how trust is formed, evolves and is exploited in a system, e.g. the trust lifecycle; how security policy can be expressed in terms of trust and access control implemented to reflect policy; and how algorithms for trust management can be implemented feasibly for a range of different applications. Further activities address these issues based on an understanding of trust derived from the formal model but also contributing to the understanding of trust as a feasible basis for making security decisions to be embodied in the model.

Fields of science (EuroSciVoc)

natural sciences > computer and information sciences > computer security > **access control**

Programme(s)

FP5-IST - Programme for research, technological development and demonstration on a "User-friendly information society, 1998-2002"

Topic(s)

IST-2001-6.2.2 - Global computing: co-operation of autonomous and mobile entities in dynamic environments

Call for proposal

Data not available

Funding Scheme

CSC - Cost-sharing contracts

Coordinator

THE PROVOST FELLOWS AND SCHOLARS OF THE COLLEGE OF THE HOLY AND UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN

EU contribution

No data

Total cost

No data

Address

COLLEGE GREEN
2 DUBLIN
Ireland

Participants (4)

AARHUS UNIVERSITET

Denmark

EU contribution

No data

Address

NORDRE RINGGADE 1
8000 AARHUS

Total cost

No data

THE CHANCELLOR, MASTERS AND SCHOLARS OF THE UNIVERSITY OF CAMBRIDGE

United Kingdom

EU contribution

No data

Address

THE OLD SCHOOLS, TRINITY LANE
CB2 1TS CAMBRIDGE

Total cost

No data

UNIVERSITE DE GENEVE

Switzerland

EU contribution

No data

Address

RUE DU GENERAL DUFOUR 24
1211 GENEVE 4

Total cost

No data

UNIVERSITY OF STRATHCLYDE

United Kingdom

EU contribution

No data

Address

RICHMOND STREET 16
G1 1XQ GLASGOW

Total cost

No data

Last update: 13 June 2005

Permalink: https://cordis.europa.eu/project/id/IST-2001-32486