Malicious- and Accidental-Fault Tolerance for Internet Applications

Fact Sheet

Project information

MAFTIA

Grant agreement ID: IST-1999-11583

Project website

Funded under:
FP5-IST

Overall budget:
€ 5 098 269

EU contribution
€ 2 499 913

Start date
1 January 2000

End date
28 February 2003

Coordinated by:
THE UNIVERSITY OF NEWCASTLE UPON TYNE

United Kingdom

Objective

The MAFTIA project will investigate the dependability of large distributed applications thus addressing one of the four key issues of the IST Programme and in particular the main objectives of CPA2. Its major innovation is a comprehensive approach for tolerating both accidental faults and malicious attacks in such systems, including attacks by external hackers and by corrupt insiders. The objectives of the project will evolve under the guidance of an Industrial Advisory Board, representing a cross-section of the industrial organizations that can best exploit MAFTIA's ideas. Board members will provide "use cases" based on actual or planned major systems and on realistic threat scenarios; as the project progresses they will play an ever-increasing role in providing exploitation routes for the results. Deliverables will include demonstrations and prototypes of several accident- and attack-tolerant security mechanisms and services.

Objectives:

MAFTIA will investigate systematically the "tolerance paradigm", to propose an integrated architecture built on this paradigm, and to realise a concrete design used to support the dependability of many applications.

MAFTIA will work on three broad categories of objectives related to:
(i) the development of an architecture ensuring the dependability of distributed applications in the face of a wide class of faults and attacks,
(ii) the design of mechanisms and protocols providing the required building blocks to implement large scale dependable applications, though four subclasses of objectives, dependable middleware, large scale intrusion detection systems, dependable trusted third parties and distributed authorisation mechanisms, and
(iii) the assessment of the basic concepts developed by MAFTIA and verifying the results of the work on dependable middleware.

Work description:
MAFTIA is structured into six technical Workpackages (WP).
WP1 will concentrate on the conceptual model and architecture of attack tolerance. The largest body of work will be carried out in designing mechanisms and protocols. This constitutes the next four work packages. The first two deal with enabling technologies while the last two are concerned with application-level technologies.
WP2 will develop a modular and scalable cryptographic group-oriented middleware suite, suitable for supporting reliable multi-party interactions under partial synchrony models and subject to malicious as well as accidental faults. We will also develop a framework for building attack-tolerant transactional systems that are as resilient to attacks as they are to accidental faults.
WP3 will investigate how Intrusion Detection Systems (IDSs) can benefit from fault injection methods, diversity from combining several systems, and distributed reasoning. The design of an IDS that is itself secure and attack-tolerant will be addressed building on results of WP2.
In WP4 we will design a generic architecture for dependable TTP services based on results from WP2. We will specify the necessary services that the TTP needs to provide, then we will implement the protocols in a first prototype and finally provide an integrated demonstrator for the TTP in the PKI scenario and in the fair exchange scenario.
In WP5, we will define a framework for access control and authorisation in a distributed environment where the access control decision is distributed among parties that might not trust each other completely. We will design and prototype flexible authorisation schemes, adapted to multi-party transactions.
The assessment and verification part forms WP6, in which we plan to work towards formalisation of the MAFTIA conceptual model, employ existing methods and tools to assess new MAFTIA mechanisms, and develop a novel combination of existing approaches to the validation of cryptographic mechanism

Milestones:
The Final Report on malicious and accidental fault tolerance for Internet applications will cover the architecture and conceptual model for the "tolerance paradigm", detailed design of dependable mechanisms and protocols, and techniques for formal assessment. Demonstrations of the prototype middleware, IDS, TTP and authorisation server will also be provided. Preliminary results (milestones) will be made available to the consortium as a whole and used to guide the work of the project.
MAFTIA fulfilled all of its original research objectives by delivering:
- a conceptual model and architecture for intrusion tolerance that bridges the gap between dependability and security;
- a set of mechanisms and protocols for achieving intrusion tolerance;
- a modular and scalable suite of middleware protocols for secure group communication;
- an architecture for a large-scale distributed intrusion detection system, which is itself intrusion-tolerant and uses a comprehensive approach to reduce the rate of false positives and false negatives;
- a blueprint for building generic trusted third-party services using state machine replication;
- the design and implementation of an intrusion-tolerant distributed authorization service;
- a model for reactive cryptographic systems that allows for formal specification and verification of security properties under a standard cryptographic semantics;
- formal verification of selected components of the MAFTIA middleware

Programme(s)

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

Topic(s)

1.1.2.-5.1.2 - CPA2: Dependability in services and technologies

Funding Scheme

CSC - Cost-sharing contracts

Coordinator

THE UNIVERSITY OF NEWCASTLE UPON TYNE
Address
6 Kensington Terrace
Ne1 7ru Newcastle Upon Tyne
United Kingdom

Participants (5)

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
France
Address
3, Rue Michel-Ange
75794 Paris Cedex 16
FUNDACAO DA FACULDADE DE CIENCIAS DA UNIVERSIDADE DE LISBOA
Portugal
Address
Campo Grande, Ed. C5
1749-016 Lisboa

INTERNATIONAL BUSINESS MACHINES CORP., RESEARCH DIVISION, T.J. WATSON RESEARCH CENTER
United States
Address
30, Sawmill River Road
10352 Hawthorne, Ny

QINETIQ LIMITED
United Kingdom
Address
85 Buckingham Gate
SW1E 6PD London

UNIVERSITAET DES SAARLANDES
Germany

Share this page

© European Union, 2019