MyThS

Models and Types for Security in Mobile Distributed Systems

IST-2001-32617

University of Sussex, Brighton
École Normale Supérieure, Paris
Università "Ca' Foscari", Venezia

Vladimiro Sassone

MyThS

Objectives:

- Type-based theories of security for mobile and distributed systems.

MyThS

Objectives:

- Type-based theories of security for mobile and distributed systems.

Focus:

- Foundational theories underpinning the design of programming languages and paradigms w static detection of security problems.

MyThS

Objectives:

- Type-based theories of security for mobile and distributed systems.

Focus:

- Foundational theories underpinning the design of programming languages and paradigms w static detection of security problems.

Results:

- Integrated set of type systems for innovative resource management and security policies, information flow analyses, and formal validation of distributed crypto-protocols.
- Rigorous design principles for secure, provably flawless systems.

MyThS' Method

MyThS unfolds in three central, challenging themes:

- *Resource access control*,
- *Information flow control*,
- *Analysis of crypto-protocols*,

MyThS' Method

MyThS unfolds in three central, challenging themes:

- *Resource access control*,
- *Information flow control*,
- *Analysis of crypto-protocols*,

focusing on two pivotal notions that traverse all themes

- *Models* (based on high-level process calculi),
- *Types* (descriptive/prescriptive, static/dynamic, with untyped components)

MyThS' Themes

Resource access control

- A calculus of capabilities with the global network's notion of access rights: enter/exit domains, cross firewalls, downgrade/upgrade agents' clearance.
- Access control with type systems to express policies based on such capabilities.
- Explore mixed static/dynamic typing, assessing the respective benefits and trade-offs between flexibility and efficiency.
- Trust management under the hypothesis of mutable clearance levels as principals travel between domain boundaries.

MyThS' Themes

Information flow control

- Study notions of information flow and non-interference, based on the new 'global computing' observables
- The focus on calculi of mobility with general forms of communication, especially with encrypted communication.
- Use type systems both prescriptively, to enforce absence of information flows, and descriptively to detect flows.
- Compare non-interference and the cause/effect relationship between agents present in well known non-interleaving concurrency models.

MyThS' Themes

Analysis of crypto-protocols

- Develop typed process calculi for modelling of security protocols: types for analysing (as opposed to specifying) properties.
- Emphasis on properties typical of e-Commerce: non-repudiation, fair-exchange, challenge-response, and attention to complexity issues.
- Apply results on information flow security: represent secrecy and authentication properties as information flows from authorised to non-authorised users.

MyThS' Workpackages

The Administration

WP0: Coordination and Contingency

WP8: Assessment and Evaluation

WP9: Dissemination and Implementation

The Research

WP1: Core Models

WP2: Typed Calculi of Capabilities

WP3: Types for Information Flow Control

WP4: Types for Protocol Analysis

WP5: Typing with Partial Knowledge

WP6: Mutable Trust and Security Levels

WP7: Programming-Level Applications

MyThS' Workpackages

The Administration

WP0: Coordination and Contingency

WP8: Assessment and Evaluation

WP9: Dissemination and Implementation

The Research

WP1: Core Models

WP2: Typed Calculi of Capabilities

WP3: Types for Information Flow Control

WP4: Types for Protocol Analysis

WP5: Typing with Partial Knowledge

WP6: Mutable Trust and Security Levels

WP7: Programming-Level Applications

The structure of WP1

WP1.1: Name-passing Models and Cryptographic primitives

WP1.2: Ambient-based Models

WP1.3: Causal Models of Information Flow

MyThS' Workpackages

The Administration

WP0: Coordination and Contingency

WP8: Assessment and Evaluation

WP9: Dissemination and Implementation

The Research

WP1: Core Models

WP2: Typed Calculi of Capabilities

WP3: Types for Information Flow Control

WP4: Types for Protocol Analysis

WP5: Typing with Partial Knowledge

WP6: Mutable Trust and Security Levels

WP7: Programming-Level Applications

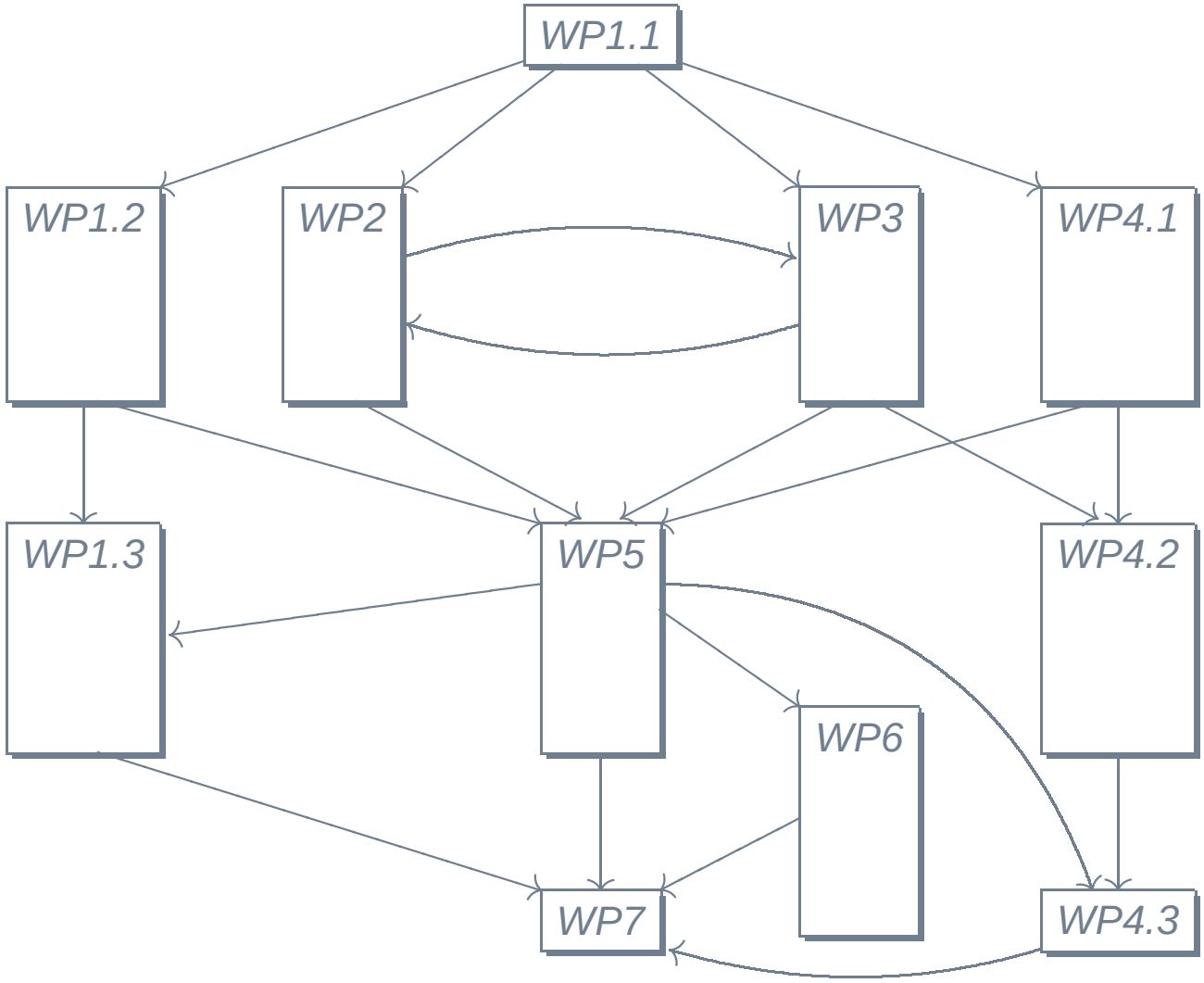
The structure of WP4

WP4.1: Basic Process Calculi

WP4.2: Network-Aware Calculi

WP4.3: Information-Flow Types for Protocol Analysis

MyThS' Activity Diagram



WP1: Core Models

Objectives

- Analyse existing models and extend them to MyThS' purposes.
- Devise new models of information flow based on causal information and related type systems.

Resp: ENS

WP2: Typed Calculi of Capabilities

Objectives

- Refine and extend the definition of resource access in the presence of mobile and migrant code.
- Devise associated notions of capabilities and primitives for managing capabilities.
- Define security policies to handle capability management.
- Introduce type systems for static access control.
- Introduce type systems to statically enforce capability management policies and detect violations.

Resp: UoV

WP3: Types for Information Flow Control

Objectives

- Define notions of flow of information determined by mobility, communication and cryptographic primitives in a distributed calculus.
- Provide definitions of information-flow security.
- Investigate notions of equivalence to capture information-flow security by means of (probabilistic) non-interference.
- Develop information-flow types and type systems for non-interference.

Resp: UoS

WP4: Types for Protocol Analysis

Objectives

- Define typed calculi and analysis for cryptographic protocols, with focus on the typed analysis of e-commerce specific protocols.
- Apply type systems for non-interference to protocol analysis.

Resp: UoV

WP5: Typing with Partial Knowledge

Objectives

- Extend typing techniques for resource management and information flow to cope with typing in the absence of centralised control.
- Balance static/dynamic techniques to maximise accuracy, expressive power, and efficiency.

Resp: UoV

WP6: Mutable Trust and Security Levels

Objectives

- Investigate the effects of agent mobility on trust level and security clearance for agents and resources.
- Develop type systems for dynamically upgrading/downgrading system and network components.

Resp: UoS

WP7: Programming-Level Applications

Objectives

- Analyse the whole project's results.
- Investigate applications to programming languages and paradigms.

Resp: ENS

MyThS' Partners

- University of Sussex

  M. Hennessy, M. Merro, J. Rathke, V. Sassone.

- École Normale Supérieure

  G. Castagna, M. Fernández, G. Longo, F. Zappa.

- Università "Ca' Foscari"

  M. Bugliesi, S. Crafa, R. Focardi