Information flow control & reputation in multiparty sessions

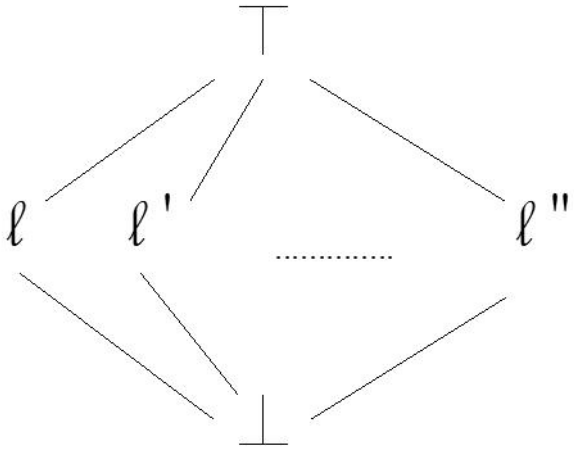
Viviana Bono
Sara Capecchi
Ilaria Castellani
Mariangiola Dezani-Ciancaglini
Tamara Rezk

Part 1
Information flow control in multiparty sessions

Data are decorated with security levels

a finite lattice of security levels

levels assigned to values and variables



Non interference: no dependency or information flow from objects of a given level to objects of lower or incomparable level

Secure information flow: the send or receive of a value v^{ℓ} can only depend on a receive or test of a value $v_0^{\ell_0}$ with $\ell_0 <= \ell$

3 ways

How to preserve data confidentiality?
How to prevent/detect information leaks?

3 ways

Typing (prevention): session type system with security

Safety (detection): induced by monitored semantics

Security (detection): behavioural property based on observational equivalence

Information leaks: example 1

$$s[1]?(2,x^{\top}).s[1]!\langle 3,true^{\perp}\rangle$$

- **Typability**: any syntactic leak is bad 
- **Safety**: any semantic leak is bad 
- **Security**: any global semantic leak is bad 

Information leaks: example 2

$$(\nu a)(a[1](\alpha).\alpha\ ?(2,x^{\top}).\ \alpha\ !<3,\mathrm{true}^{\perp}>)$$

- **Typability**: any syntactic leak is bad 
- **Safety**: any semantic leak is bad 
- **Security**: any global semantic leak is bad 

Information leaks: example 3

$$\text{if } \text{true}^{\top} \text{ then } s[1] !< 2, \text{true}^{\bot} \text{ else } s[1] !< 2, \text{false}^{\bot}$$

- **Typability**: any syntactic leak is bad 
- **Safety**: any semantic leak is bad 
- **Security**: any global semantic leak is bad 

Relating the three properties

Typability

+ declassification
+ access control

Security

Session Types for Access and Information Flow Control
Capecchi Castellani Dezani-Ciancaglini Rezk
Concur 2010

Typing Access Control and Secure Information Flow in Sessions
Capecchi Castellani Dezani-Ciancaglini
Information and Computation, to appear.

Relating the three properties

Typabilty

Safety

Security

Information Flow Safety in Multiparty Sessions
Capecchi Castellani Dezani-Ciancaglini
Express 2011 + Mathematical Structures in Computer Science (to appear)

Part 2
A reputation system for multiparty sessions

Starting point

dynamic multirole sessions (Deniélou,Yoshida)

service vs session

histories of principals

policies

A Reputation System for Multirole Sessions

Bono Capecchi Castellani Dezani-Ciancaglini

TGC 2011

Service vs Session

Service: an abstraction of a multiparty interaction point playing predefined roles and behaving w.r.t. a protocol

Session: instantiation of a service

Stable vs one shot join

Histories

Trace of past interactions in service sessions
(history of a participant in a role w.r.t. a service)

Two send constructs: ! • !

Histories are used:

- at service join
- at session initiation
- poll operation

Policies

Used to check reputations:

- by a service to select participants for a given role
- by participants to:
  - decide whether to join a service
  - select participants in a poll operation