Compositional Verification of Secure Applet Interaction

Dilian Gurov
- SICS -

Marieke Huisman, Gilles Barthe
- INRIA Sophia-Antipolis -

Overview

- Motivation
- Background
- Compositional Approach
- Conclusion

Purpose of the Presentation

Summarize the results obtained and the work-in-progress in WP4 concerning *compositional applet verification*.

Motivation

Prospect of *post-issuance loading* of applets in *multi-application* smartcards: compositional reasoning techniques required.

Compositional Approach

Decompose global, smartcard-wide properties to local properties of the individual applets. Tasks involved:

- finding suitable local properties
- proving the decomposition correct
- verifying the individual applets.

Background

Approach 1 [Jensen *et al* '99]

- control-flow graph G
- state: sequence of vertices (call stack)
- operational semantics: trace semantics induced by transition rules
- security properties: call-stack invariants
- model checking: property-specific, property-preserving abstraction.

Approach 2 Context-Free Processes

- productions $v \to p$ induced by G

- state: sequence of vertices

- operational semantics:
  - prefix transition rule

- security properties:
  - specified in *temporal logic*
  - denote computation sequences or trees

- model checking: polynomial in the size of the CFP [Burkart & Steffen '92].

Extension to Boolean programs: pushdown systems [Esparza & Schwoon '01].

Approach 3 Compositional Reasoning about Interaction Behaviour [Dam *et al.* '98]

- hierarchy of *components*:
  - data
  - functions/expressions
  - processes

- compositional labelled-transition semantics

- specification language: modal logic with recursion (modal μ-calculus)

- proof system:
  - Gentzen sequents with *parameters*
  - transition proof rules
  - fixed-point induction

- verification: proof-assistant (EVT).

Compositional Approach to Applet Verification

A. Compositional Program Model

- control-flow graph G with *applet regions*

- state:
  - local: sequence of vertex pairs
  - global: well-formed set of local states

- operational sematics: LTS
  - actions: input/output/perfect, call/return
  - action-labelled transitions
  - local transition rules
  - synchronization on transition labels

B. Properties of Interaction Behaviour

- underlying logic: modal μ-calculus augmented with model-specific features. Allows the encoding of higher-level property constructs ("patterns")

- safety properties: strictly more expressive than Jensen's logic

- model checking: decidable for CFP, but of a higher complexity

C. Compositional Proof System

- Gentzen sequents with parameters
- transition proof rules
- fixed-point induction

- soundness: checked in PVS
- completeness/decidability?
- tool support: adapting the EVT
- efficient automatic techniques: product formulae?

D. Model Checking Local Properties

- extracting control-flow graphs, or directly CFP productions, by using existing techniques and tools

- translating properties into the (pure) modal μ-calculus

Conclusion

Achieved

- compositional program model
- property specification language
- proof system for property decompositions

In Progress

- tool support
- case studies, properties
- completeness and automation issues
- model checking local properties

Future Work

Extensions for dealing with:
- data: Boolean programs?
- multi-threading?