Verification of Secure Applet Interaction

(Abstract)

Dilian Gurov
Swedish Institute of Computer Science

Gilles Barthe, Marieke Huisman
INRIA Sophia-Antipolis

We propose to present a summary of the results obtained, and the work-in-progress in WP4 concerning *compositional applet verification*. The development of compositional specification and verification techniques is motivated by the prospect of post-issuance loading of applets in multi-application smart cards.

Two existing frameworks for the verification of the procedure-call behaviour of programs form the background for our research. The first framework, developed by Jensen and others, consists of a program model based on a transfer/call control-flow graph and a notion of state being represented as a sequence of nodes in this graph (call-stack), a property specification language for specifying security properties as invariant properties of the program's call-stack, and a technique for faithful abstraction allowing a property to be checked on a finite prefix of the (possibly infinite) computation-tree. The second framework models the procedure-call behaviour of programs in terms of *pushdown systems*, uses temporal logic for expressing behavioural properties, and algorithmic techniques for checking these (the model-checking problem is decidable in this case).

Our approach combines ideas from the above frameworks in a compositional setting. We adapt Jensen's program model by adding applet interaction in a process-algebraic style through transition labels and synchronisation on these, in this way capturing the interaction (interface) behaviour of the individual applets and composing these behaviours into the global behaviour of the applet set. Security properties are then expressed in a suitable extension of the modal μ-calculus as properties of the interaction behavior. In this way we obtain a wider class of properties, with a model-checking problem of a correspondingly higher complexity, than in Jensen's approach. The properties of the applet set are to be decomposed into properties of the individual applets. We provide a Gentzen sequent calculus-style proof system for proving correctness of property decompositions. The individual applet properties are then to be model-checked by translating the model into the language of *context-free processes* - a subclass of pushdown-systems allowing more efficient model-checking - and the properties to modal μ-calculus formulae.

We shall also discuss tool support, case studies, and the future efforts planned in this track.