Proof compression and the Mobius PCC architecture for embedded devices

Thomas Jensen
CNRS
IRISA, Campus de Beaulieu, F-35042 Rennes, France

The EU Mobius project[1] has been concerned with the security of Java applications, and of mobile devices such as smart phones that execute such applications. In this talk, I'll give a brief overview of the results obtained on on-device checking of various security-related program properties. I'll then describe in more detail how the concept of certified abstract interpretation and abstraction-carrying code can be applied to polyhedral-based analysis of Java byte code in order to verify properties pertaining to the usage of resources of a down-loaded application. Particular emphasis has been on finding ways of reducing the size of the certificates that accompany a piece of code.

Such analyses will produce program invariants in the form of fixpoints of abstract transfer functions and the present work has been concerned with several aspects of how to simplify and reduce the size of these fixpoints:

- Abstract interpretations will often produce more information that necessary for proving a particular program property. I will introduce the notion of a **witness** of a property together with a technique for **pruning** program invariants to provide the minimum information necessary to prove a particular property.
- In the context of polyhedral-based abstract interpretation, an essential part of verifying a proposed invariant is the checking of polyhedral inclusions. I'll describe a notion of certificate for checking polyhedral inclusions based on a use of Farkas' lemma that reduces inclusion checking to a few simple matrix computations.
- The checking of a proposed invariant involves a certain amount of re-computing the invariant. It is therefore possible to reduce the amount of information that is being transmitted in the certificate because the checker will reconstruct it anyway. This leads to general **fixpoint reconstruction** algorithms that generalize the dedicated algorithms from lightweight bytecode verification.

Checkers of such compressed certificates have been developed in the proof assistant Coq and extracted to be executed on several types of mobile devices.

References

Eva Rose. Lightweight bytecode verification. *J. Autom. Reason.*, 31(3-4):303–334, 2003.

Frédéric Besson, Thomas Jensen, and David Pichardie. Proof-Carrying Code from Certified Abstract Interpretation and Fixpoint Compression. *Theoretical Computer Science*, 364(3):273–291, 2006.

Frédéric Besson, Thomas Jensen, Tiphaine Turpin. Small witnesses for abstract interpretation based proofs. In *Proceedings of the 16th European Symp. on Programming (ESOP 2007)*, Springer LNCS vol. 4421, 2007.

E. Denney, T. Jensen (eds.); The 3rd International Workshop on Proof Carrying Code and Software Certification, pp. 33-33

[1]This work was partialy supported by the EU FET project FP6-015905 Mobius