Flow Logics for Carmel

René Rydhof Hansen*

Informatics and Mathematical Modelling, building 321
Technical University of Denmark, DK-2800 Lyngby, Denmark
E-mail: `rrh@imm.dtu.dk`

Java Card is a specialised version of Java, intended for the programming of "Java cards", which are smart cards with an on-card Java Card Virtual Machine. Java Card is translated into Java Card Virtual Machine Language (JCVML), the java card equivalent of Java Virtual Machine Language, before it is downloaded onto a java card and executed by the Java Card Virtual Machine. Carmel is a complete subset of the JCVML. Complete in the sense that all instructions from the "real" JCVML specification are either directly represented in Carmel or can be simulated by the Carmel instruction set, eg. all JCVML instructions that push a specific constant are simulated by the generel push construction of Carmel. This leads to a relatively small and manageable programming language, more amenable to formal methods and static analysis than the JCVML.

We introduce the Carmel language and discuss the relationship between JCVML and Carmel; also briefly discussed are some of the features and "curiosities" of JCVML, and indeed Carmel, that arise from the fact that these langauges are used to program java cards. Furthermore we present a Control Flow Analysis (CFA) for Carmel, specified in the Flow Logic framework of Nielson and Nielson. The CFA is proved semantically correct with respect to a small step operational semantics; this is done by establishing a subject reduction property for the CFA as is usual in the Flow Logic framework. A few interesting cases from the proof are shown and the semantics necessary to do so is introduced.

Finally, implementation issues and possible applications of the analysis are discussed; in particular how the analysis might be used for validating certain security properties of Carmel programs.

*Funded by the SecSafe project (EU research project)