Finding Security Bugs in Java Programs Using Datalog

Bernhard Scholz, Nicholas Allen and Padmanabhan Krishnan
Oracle Labs,
Brisbane, Australia
Email: {bernhard.scholz,nicholas.allen,paddy.krishnan}@oracle.com

Recently, various zero-day exploits emerged for Java making computers that run Java potentially vulnerable. Though Java was designed with a strong emphasis on security and the language itself is type-safe, defects in the Java JDK library permit attackers to break the security of Java. This talk gives an overview of the activities at Oracle Labs that has been developing a program analysis tool for Java and the JDK library.

The program analysis tool will be able to identify and report security defects in the JDK library. In a pilot project, we specify security defects of Java programs in a restricted variant of Horn-Logic called Datalog. The declarative approach of expressing static program analyses has various advantages.

The main features include building a global analysis for incomplete programs, a suitable points-to relation to identify tainted input and data-flow analysis to check permissions on certain paths. The results of our pilot project will be summarised.