

Security policy verification via information flow analysis

Abstract

Many security properties of programs describe requirements on actions with data (e.g., "No SQL injection"). Simple inspection of method calls without taking into account the data involved results in an over-approximation and can produce a false verification results. To improve the precision of the verification of security requirements, we propose to track data flow inside the program implementation. This tracking is achieved through taint analysis. In taint analysis, security-relevant data (chosen by the user) is assigned a label called taint that travels through the program execution along with the data. The taint analysis with the security property makes the verification precise. To implement this new analysis, we propose an addition to JPF that allows users to check programs against security specifications that mandate proper sequencing on actions and data in order to conform with security standards.

Contact

student: Anton Philippov <anton.e.philippov AT gmail.com>

mentor: Eric Mercer <recremcire AT gmail.com>

co-mentor: Peter Mehlitz <pcmehlitz AT gmail.com>, Oksana Tkachuk

Repository

[jpf-security](https://bitbucket.org/jpf-security) is hosted on <https://bitbucket.org/>

Description

Project documentation/wiki/blog are available at the [jpf-security respository](#)