IPSJ Transactions on Programming Vol.8 No.3 37 (Sep. 2015)

Abstract

Generating Stack-based Access Control Policies

Xin Li[1,a) Hua Vy Le Thanh[2]

Presented: March 9, 2015

The stack-based access control mechanism plays a fundamental role in the security architecture of Java and Microsoft CLR (common language runtime). It is enforced at runtime by inspecting methods in the current call stack for granted permissions before the program performs safety-critical operations. Although stack inspection is well studied, there are relatively little work on automated generation of access control policies. Practiced approaches to generating access control policies are still manually done by developers based on domain-specific knowledges and trial-and-error testing. In this paper, we present a systematic approach to automated generation of access control policies for Java programs that necessarily ensure the program to pass stack inspection. The techniques are context-sensitive static program analyses based on abstract interpretation. Our analysis models the program by combining a context-sensitive call graph with a dependency graph. We are hereby able to precisely identify permission requirements at stack inspection points, which are usually ignored in previous study.

[1] The University of Tokyo
[2] University of Science — Ho Chi Minh City
[a)] li-xin@kb.is.s.u-tokyo.ac.jp

© 2015 Information Processing Society of Japan