Title: 05_oopsla_ Finding Application Errors and Security Flaws Using PQL: a Program Query Language

Author: Michael Martin Benjamin Livshits Monica S. Lam

Background:
A number of effective error detection tools have been built in recent years to check if a program conforms to certain design rules. An important class of design rules deals with sequences of events associated with a set of related objects.

Conclusion:

1. This paper presents a language called PQL(Program Query Language) that allows programmers to express such questions easily in an application-specific context.
2. We have developed both static and dynamic techniques to find solutions to PQL queries.

Method:

1. The focus of PQL is to track method invocations and accesses of fields and array elements in related objects. Design a query language.
2. Model the dynamic program execution as a sequence of primitive events, in which the checkers find all subsequences that match the specified pattern.
3. Using static analysis to optimize the result

Useful Information:

1. Semantic of the language:
    1. altStmt = a or b
    2. within = allow the specification of a pattern to fully match within a invocation of a method
    3.

Useful Related Work:

Referenced statements:

1. As an example, let us consider SQL injection vulnerabilities[5, 27], ranked as one of the top five external threats to cooperate IT system[52].
2. Despite being garbage collected, Java programs can still have memory leaks[51].