発表概要

データフロー解析結果を付加した構文木に対するパターンマッチによるコード検査

谷口 力斗[1,a)]　馬谷 誠二[2,b)]　鵜川 始陽[3,c)]

2017年3月3日発表

プログラマはセキュアコーディング規約や，ライブラリの API に従わなければならない．規約に従わないプログラムは脆弱性を引き起こしたり正しく動作しないこともある．そのため，ソースコードを検査してコーディング規約や API の違反を検出するツールが開発されている．我々が開発を行っている ASTgrep もその 1 つである．ASTgrep は，C プログラムを S 式で表現された抽象構文木（S-AST）に変換するフロントエンドと，同じく S 式で表現される違反コードパターンとフロントエンドが生成する S-AST とのパターンマッチを行うバックエンドからなる．しかし，ソースコードの構文的な特徴を反映しただけの S-AST では，null 参照のようなデータフローを考慮する必要のあるパターンを表現できない．そこで，本研究では ASTgrep を改良し，データフロー解析の結果を S-AST に付与し，データフローに依存する違反パターンを表現可能にする．改良した ASTgrep は，LLVM を使ってデータフロー解析を行い，その結果をフロントエンドから生成される S-AST に付与する．改良前の ASTgrep では記述できなかったセキュアコーディング規約のいくつかを，改良後の ASTgrep を用いて実際に記述・検出できることを確認した．

Checking Code by Pattern Matching against Abstract Syntax Trees Enriched with Data-flow Information

Rikito Taniguchi[1,a)]　Seiji Umatani[2,b)]　Tomoharu Ugawa[3,c)]

Presented: March 3, 2017

Programmers must follow coding rules such as the secure coding standard and API of libraries that they use. Otherwise, programs may cause vulnerability or may not work properly. Therefore, source code checking tools have been developed to detect violations of coding rules or APIs. ASTgrep takes patterns of code fragments that violate rules as well as the source code to be checked, so it can detect violations of varieties of rules. It consists of two parts, the frontend and the backend; the frontend converts a C program into an abstract syntax tree represented in an S-expression (S-AST). The backend pattern matches between the pattern, which is also written in an S-expression and the S-AST generated by the frontend. Since the S-AST reflects only the syntactic information of the source code, it was not possible to express patterns of violations that depend on data-flow information, e.g., patterns of null dereferences. Therefore, we improved ASTgrep by enriching the S-AST with data-flow information so that we can express patterns that depend on data-flow information. Our improved ASTgrep performs data-flow analysis by using LLVM, and attaches its result to the S-AST. With the improved ASTgrep, we successfully described patterns and detected violations of some secure coding rules that we failed to detect with the previous ASTgrep.

[1] 京都大学工学部情報学科
Undergraduate School of Informatics and Mathematical Science, Faculty of Engineering, Kyoto University, Kyoto 606–8501, Japan
[2] 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University, Kyoto 606–8501, Japan
[3] 高知工科大学
Kochi University of Technology, Kami, Kochi 782–8502, Japan

[a)] taniguchi@fos.kuis.kyoto-u.ac.jp
[b)] umatani@kuis.kyoto-u.ac.jp
[c)] ugawa.tomoharu@kochi-tech.ac.jp