発表概要

静的解析を用いたWebアプリケーションの脆弱性検出の一手法

西田誠幸†

近年，SQL インジェクションやクロスサイトスクリプティングなどの脆弱性を突いた Web アプリケーションへの不正アクセスが問題となっている．これらの脆弱性は，Web アプリケーションを構成するプログラムが，ユーザ入力文字列に対するエスケープ処理を怠って HTML 文書や SQL 文の一部として出力することによって起こる．本発表では Web アプリケーションを構成する手続き型言語のプログラムを静的に解析して，プログラム中の脆弱性の存在を検出する一手法を提案する．この手法では，プログラムの手続きを単位として，入力文字列の伝播を表す関数を生成する．そしてプログラム中のすべての手続きに対して得られる入力文字列伝播関数を解決することによって脆弱性を検出する．すなわち，入力文字列が出力文字列の一部として伝播すると判断されたとき，対象のプログラムに脆弱性が存在すると見なす．本手法は，プログラムの手続きを，その呼び出し元とは独立に解析する．したがって，1 つの手続きの解析の手間は，その呼び出し回数に支配されない．また MVC フレームワークやテンプレートなど，複数の言語を使って構成される Web アプリケーションについて，各言語の手続きから関数を生成する処理の間の関連がたがいに疎であるため，それぞれの処理を分割して実装することが可能である．一方，これらの各処理によって得られる関数を解決する処理は，対象とする言語とは独立に実装可能である．

A Static Analysis for Detecting Web Application Vulnerability

Seikoh Nishita†

We propose a technique for detecting the vulnerability of Web applications such as SQL injection and cross-site scripting by static analysis of procedural language programs that compose the Web applications. Our technique inputs procedures of the programs as a unit, and generates some functions that represent the input character string propagation. And, it detects the vulnerability by resolving the functions obtained from all procedures in the programs. That is, our technique inform the existence of the vulnerability when the resolved functions suggests that the input character string propagates to the part of output text such as HTML documents and SQL commands. Our technique analyzes the procedures independently of the procedural calls. Therefore, the number of procedural calls is not occupied in the complexity of the analysis for the procedure. Moreover, when the Web application is composed by two or more languages by techniques such as MVC frameworks and templates, each processing of function generation for the languages can be implemented separately, because the function generation processing of each language is mutually related loosely. On the other hand, the resolver of the functions is implemented independently of the target languages.

（平成 18 年 10 月 13 日発表）

† 拓殖大学工学部情報工学科
Department of Computer Science, Takushoku University