要 旨

ルールに基づくバッファオーバーフロー脆弱性自動検出法に関する研究

浦部未来

ソフトウェアに潜在する脆弱性の一つとしてバッファオーバーフローが挙げられる．ソフトウェア記述言語として普及している C 言語ではメモリ管理がプログラマに任されているため，バッファオーバーフローが起こる可能性が高く，バッファオーバーフローに対する対策が重要である．C 言語プログラムに対するバッファオーバーフローの検出に関して，Shahriar らの研究では，バッファオーバーフローになりうるプログラムのパターンと，それを安全なコードに書き換えるルールが提案されている．そのルールに従ってプログラムソースを検査し，検出箇所を書き換えることによって，バッファオーバーフローの発生を抑えられることを実験的に示している．しかし，この研究では検出・書き換えを全て手動で行うものとなっており，その自動化が課題とされていた．

そこで，本研究では，Shahriar らのバッファオーバーフロー検出のルールに基づき，C 言語で書かれたプログラムソースからルールに該当する箇所を自動で検出するシステムを構築する．

結果，ルールの一部において自動化を行い，検出を確認した．

今後の課題として，残りのルールの自動化実装，書き換え部分の自動化，静的解析などによる誤検出の低減が挙げられる．

キーワード　バッファオーバーフロー，C 言語

Abstract

Rule-Based Automatic Detection of Buffer Overflow Vulnerability

Miki Urabe

Buffer overflow (BOF) is one of the most important software vulnerability. The C programming language which is popular as a software description language, is a high possibility of buffer overflow because the programmer consider must the memory management. Therefore, buffer overflow protection is important and measures to protect the C program from the buffer overflow is important.

Shahriar et al. proposed a rule-base detection and patching method of BOF vulnerabilities. However, in this approach the programmer should apply the proposed patching rules manually. Developing an automated tool for applying the rules is desired.

In this study, we build an automatic detection system that finds a buffer overflow vulnerability using Sharriar's rules.

We implemented some of the rules and confirmed that our system automatically detected a number of known vulnerabilities in open source software.

The future work includes automation of the rest of the rules, automation of patching, and reduction of false positives using static analysis.

key words Buffer overflow, C programming langrage