大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

Concolic testingツールKLEEの メモリ関連バグ発見能力の評価

株式会社 日立製作所 鈴木貴敦 takanobu.suzuki.ef@hitachi.com
株式会社 デンソー 黄文鴻 wenhungi.huang.j5y@jp.denso.com

開発における問題点

- メモリ関連バグはソフトウェア脆弱性の7割を占める
- 特に多いのは、領域外アクセス

手法・ツールの適用による解決

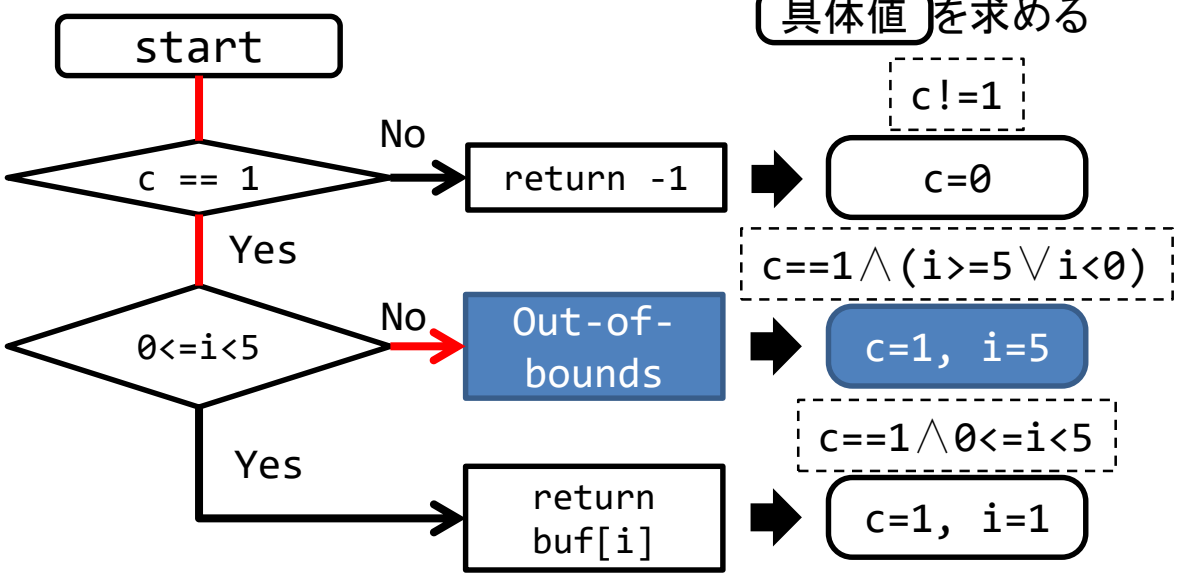
- メモリアクセス実行時に、アクセス範囲を網羅的にチェックするConcolic testingツールKLEEでメモリ関連バグを発見する
- 目標：KLEEのバグ発見能力評価

KLEEによるバグ発見の流れ

(1)ソースコードをLLVM bitcodeに変換

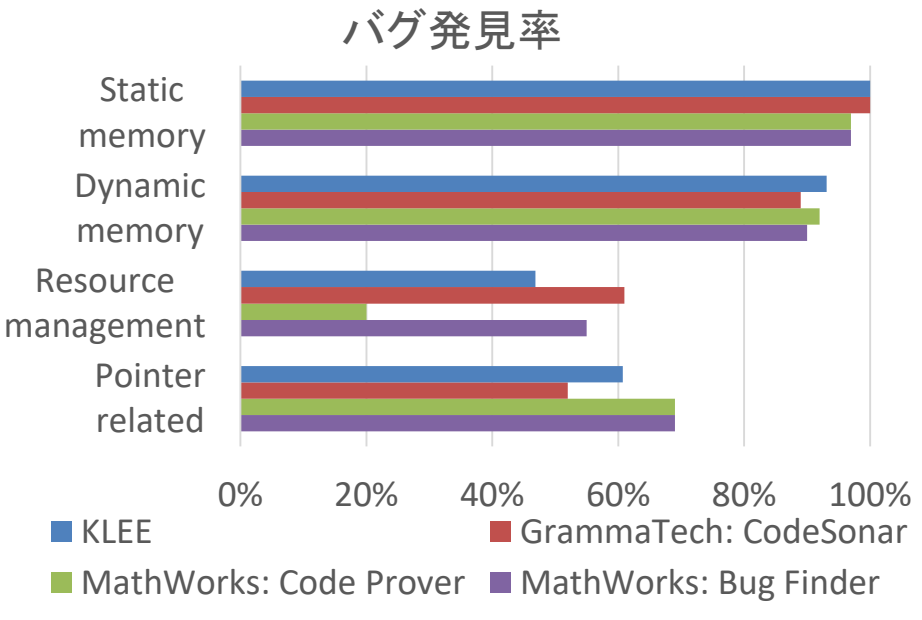
```
int buf[5];
int out_of_bounds
    (int c, int i)
{
  if (c == 1)
    return buf[i];
  else
    return -1;
}
```

(2)実行パス抽出し、網羅実行



(3)各結果への 到達条件 と 具体値 を求める

バグ発見能力評価・考察



- 静的解析ツール*1のベンチマークで評価実施
- KLEEのメモリバグ発見能力は商用ツールと遜色なし。特に、領域外アクセス(左図Static memory、Dynamic memoryと関連)は90%以上の発見率達成。
- KLEEの短所はメモリリーク(左図Resource Managementと関連)を発見できない点。対策は、メモリリークを発見できる別ツールと併用すること。

(*1) S. Shiraishi, et al., “Test Suites for Benchmarks of Static Analysis Tools”, 2015 IEEE ISSRE Workshop