Resumo do artigo Invariantes perigosas

Fábio Moreira Duarte

Sumário

1 Introdução 3
2 De contra exemplos a variantes de perigo 4
2.1 De segurança ao perigo 4

Resumo

Analisadores estatisticos procuram provas sobre-aproximadas de segurança conhecidas como invariantes de seguranca. Tais analisadores resumem tracos em conjuntos de estados, negociando a habilidade de distinguir tracos para traficabilidade computacional. Localizadores de erro estatisco, dado evidencia da falha de um afirmação, por contra exemplo. Localizadores de erro falham escalando quando analisam programas com erros que requerem muitas iterações ou laços com o esforco computacional crescendo exponencialmente com a profundidade do erro. É proposto o conceito de invariantes de perigo, setam o conjunto de traços que garantidamente chegaram a um estado de erro. Permite encontrar erros profundos sem alarme falso sem desenrolar laços.

1 Introdução

Analisadores de segurança procuram por provas de segurança conhecida como invariantes de segunraca sobre-aproximando o conjunto de estados do programa, alcansado durante toda execução do programa. Resumem traços em estados abstratos, trocando a habilidade de distinguir tracos para rastreabilidade computacional. Analisadores de segurança podem gerar relatorios de erros que não correspondem ao erro no codigo. Alarme falso são barreiras primarias para adoçao de tecnologia de analise estatistica fora das universidade. Distinguir entre erros verdadeiros ou alarme falsos é uma dificil tarefa.

Localizadores de erros estatistico como checagem de modelos delimitados busca por provas que podem ser violadas seguramente. Tem a propriedade atrativa que quando uma afirmação falha, um contra exemplo é retornado, podendo ser inspecionado pelo usuario. O contra exemplo prova que uma violação da afirmativa pode ocorrer. Para contruir tais provas, modelos de checagem delimitada computam as subsequentes aproximações do programa de estados atraves do avanço progressivo da relações de trasição. Localizadores de erros estatisticos falham na escala quando analisam programas com erros que requerem muitas iterações de um laço. O esforco computacional requerido para descobrir a violação da afirmação, cresce exponencialmente.

Abordagens baseadas em combinatoria de sobre e sob aproximações são não otimizadas para busca profunda. Pois podem apenas detectar contra exemplos com laçõs profundos apos refutação repetida de contraexemplos espurios cada vez mais longos.

Prova do perigo: No artigo propoem-se uma representação da prova baseada em sintese de rastreamento. Propoe a junção de dois nucleos conceituais baseados em analise de segurança em interpretações abstratas e localizadores de erro.

Sintese de rastreamento é uma dupla de invariantes segurança, referindo-se a invariantes de perigo. Invariantes de perigo não alcansam todos os estados do programa, mas deve conter ao menos uma execução de rastreamento viável. Um invariante de perigo pode englobar multiplos caminhos do programa, contem informações para direcionar a leitura concreta de rastreamento de erro.

Invariantes de perigo permite o desenvolvedor utilizar tecnicas de localização de falhas que não requerem desenrolamento de laços. Melhora a escalabilidade de busca de falhas, permitindo a detecção de falhas profundas.

2 De contra exemplos a variantes de perigo

Representa um programa P como um sistema de transições com espaço de estado X e relações de transições T contem X vezes X. Para o estado x existe X com T(x,x'), x' é o sucesso de x sobre T. Denota o estado inicial como I e estados de erro como E.

Definição 1(rastreabilidade da execução): Um programa de rastreamento (x0 ... xn) é (potencialmente infinito, em casos onde n = w) sequencia de estado, quaisquer dois estados sucessivos são relatados pelo programa de transição de relação T.

Definição 2(contra exemplo): Um ratreador de execuções finitas é um contra exemplo, se x0 é o estado inicial, xo existe I, e xN é estado de erro, xn existe E.

Definição 3(Invariantes de segurança): Um predicado S é invariante de segurança para o Laço L (I,G,T,A) se satisfeito os criterios.

Existe X.I(x) -¿ S(x) Existe X,X'.S(X) and G(x) and T(x,x') -¿ S(x') Existe x.S(x) and não G(x) -¿ A(x)

2.1 De segurança ao perigo

A definição 3 captura a noção de invariante de segurança. Considera-se que a noção dupla de invariante de segurança parece, e identifica os criterios que definiem-a.