Juliana Carpes Imperial

Técnicas para o Uso do Cálculo de Hoare em PCC

DISSERTAÇÃO DE MESTRADO

DEPARTAMENTO DE INFORMÁTICA
Programa de Pós-Graduação em Informática

Rio de Janeiro
Agosto de 2003

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Juliana Carpes Imperial

Técnicas para o Uso do Cálculo de Hoare em PCC

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Informática da PUC-Rio.

Orientador: Prof. Edward Hermann Haeusler

Rio de Janeiro, agosto de 2003

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Juliana Carpes Imperial

Técnicas para o Uso do Cálculo de Hoare em PCC

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-Graduação em Informática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Edward Hermann Haeusler
Orientador
PUC-Rio

Prof. Paulo Augusto Silva Veloso
COPPE/UFRJ

Prof. Christiano de Oliveira Braga
UFF

Prof. Mario Roberto F Benevides
COPPE/UFRJ

Prof. Ney Dumont
Coordenador Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 14 de agosto de 2003

Juliana Carpes Imperial

Graduou-se em Engenharia de Computação na PUC-Rio (Pontifícia Universidade Católica do Rio de Janeiro) em julho de 2001. Sua área de pesquisa é a de Teoria da Computação, tendo participado de alguns congressos e seminários em sua área de atuação.

Ficha Catalográfica

Imperial, Juliana Carpes

Técnicas para o uso do cálculo de Hoare em PCC / Juliana Carpes Imperial; orientador: Edward Hermann Haeusler. – Rio de Janeiro: PUC-Rio, Departamento de Informática, 2003.

137 f. : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática

1. Informática – Teses 2. Cálculo de Hoare. 3. Programação (Computadores). 4. Programas de computador – Medidas de segurança. 5. Lógica computacional. 6. Invariantes de Loops. I. Haeusler, Edward Hermann. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

DDD: 004

Agradecimentos

A Deus por ter me permitido concluir esse trabalho e ter me dado a chance de possuir todo o conhecimento que tenho hoje.

Aos meus pais, por durante muitos anos terem investido em mim para que eu pudesse estudar nas melhores instituições de ensino e, desta forma, adquirisse as ferramentas necessárias para facilitar meu aprendizado.

Ao Hermann, meu orientador, por sempre ter sido atencioso comigo tanto na elaboração deste trabalho quanto durante as aulas nas quais ele foi meu professor, sempre disposto a tirar minhas dúvidas e por ter me ensinado boa parte do que sei em minha área de pesquisa.

A todos os professores do departamento de Informática, por tudo o que me ensinaram e por toda atenção que sempre me dedicaram.

A todos os funcionários do departamento de Informática, por sempre estarem dispostos a ajudar e pela simpatia.

À CAPES, à FAPERJ e à PUC-Rio, pelos auxílios concedidos, sem os quais este trabalho não poderia ter sido realizado.

Aos professores que participaram da Comissão Examinadora.

Aos meus colegas e amigos do TECMF que sempre me apoiaram e ajudaram quando eu precisava.

A todos os meus colegas e amigos de pós-graduação que conviveram comigo, em especial para Carlos de Salles, Claudio de Biasi, Elton Silva, Fabio Marcos, Renato Maia, Ronaldo Luiz e Sergio de Biasi.

Aos meus gatos Tigresa, Billy e Nicky que sempre me fizeram companhia durante os meus estudos e na elaboração desta dissertação, especialmente a primeira, que muitas vezes ficava no meu colo durante tais tarefas pedindo carinho.

Resumo

Imperial, Juliana Carpes. **Técnicas para o Uso do Cálculo de Hoare em PCC.** Rio de Janeiro, 2003. 135p. Dissertação de Mestrado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Atualmente, a maioria dos programas para computadores é obtida através da WEB. Como muitas vezes a procedência são fontes desconhecidas, é preciso se certificar de que o código se comporta como o esperado. A solução ideal seria verificar o código contra uma especificação de políticas de segurança, contudo, isso pode consumir muito tempo. Uma outra alternativa é fazer com que o próprio código prove ser seguro. O conceito de *proof-carrying code* (PCC) é baseado nessa idéia: um programa carrega consigo uma prova de sua conformidade com certas políticas de segurança. Ou seja, ele carrega uma prova a respeito de propriedades do próprio código. Portanto, os mesmos métodos formais usados para a verificação de programas podem ser utilizados para esta tecnologia. Considerando este fato, neste trabalho é estudado como o cálculo de Hoare, um método formal para realizar a verificação de programas, aplicado a códigos-fonte escritos em uma linguagem de programação imperativa, pode ser útil à técnica de PCC. Conseqüentemente, são pesquisados métodos para a geração de provas de correção de programas utilizando o método citado, para tornar possível a geração de provas de segurança para PCC utilizando o cálculo de Hoare.

Palavras-chave

Proof-Carrying code; Cálculo de Hoare; Correção de Programas; Segurança; Lógica de Primeira Ordem; Invariantes de Loops; Prova de Teoremas; Prolog

Abstract

Imperial, Juliana Carpes. **Techniques for the Use of Hoare Logic in PCC.** Rio de Janeiro, 2003. 135p. MSc. Dissertation - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

Nowadays most computer programs are obtained from the WEB. Since their source is usually unknown, it is necessary to be sure that the code of the program behaves as expected. The ideal solution would be verify the code against a specification of safety policies. However, this can take too much time. Another approach is making the code itself prove that it is safe. The concept of proof-carrying code (PCC) is based on this idea: a program carries a proof of its conformity with certain safety policies. That is, it carries a proof concerning properties related to the code itself. Therefore, the same formal methods employed in formal verification of programs can be used in this technology. Due to this fact, in this work it is studied how Hoare logic applied to source codes written in an imperative programming language, which is a formal method to verify programs, can be useful to PCC. Consequently, methods are researched to generate proofs of program correctness using the method explained, so that it can be possible to generate PCC safety programs with Hoare logic.

Keywords

Proof-Carrying code; Hoare Logic; Program Verification; Safety; First Order Logic; Loops' Invariants; Theorem Proving; Prolog

Sumário

Lista de figuras