

Milestone Talk
PLaSSE Research in 2011

도경구

한양대학교 ERICA캠퍼스
PLaSSE Research Laboratory

2011년 6월 26일
파주 지지향

PLASSE
RESEARCH

Theme

ROSAEC Theme

- Software Analysis for Error-free Computing
- Team 1: Leading analysis technology research & development
- Ours: Automatic extraction of properties from programs

PLaSSE Research Theme

- Programming Language theory & technology
 - applied to Software Security
 - applied to Software Engineering
- to enhance the quality & security of software
- will develop "good" tools to guide programmers

Clone Detection

AST-based Clone Detection

- define clone as "structural pattern"
- anti-unification algorithm
- motto: no false positive, no false negative
- implementation: Code Clone Ransacker (CCR)
- evaluation versus CloneDR
 - runs 2.5-6 times slower (up to 200,000 loc)
 - finds 2-3 times more clones

Automatic Creation of Code-clone Reference Corpus

- Bellon's manual list of reference corpus
- CCR's recall ratio: 94-100%
- CCR found 2-5 times more

Abstract Parsing

Methodology matured

- basic idea developed, implemented and experimented
- dealing with destructive string operator
- modular abstract parsing
- scanner composed into parsing
- semantic processing

Application abundant

- static validation of dynamically generated HTML documents
- reconstruction of database schema from database applications
- static detection of injection vulnerabilities
- and more ...

Theory being polished

웹응용소프트웨어 보안취약성 정밀진단 기술 개발

- 산학연협력 기업부설연구소 업그레이드 지원사업 (중소기업청지원)
- 기업: 지티원(주)
- 연구개발 목표
 - (정적분석) 요약파싱을 이용한 정밀진단 기술의 개발 및 실현
 - (정적분석) 정밀 침투시험기 설계 및 구현