REFACTORERL PROJECT SUMMARY

ISTVÁN BOZÓ, MELINDA TÓTH

Application Domain Specific Highly Reliable IT Solutions project has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme.

National Research, Development and Innovation Office
Hungary

PROGRAM FINANCED FROM THE NRDI FUND

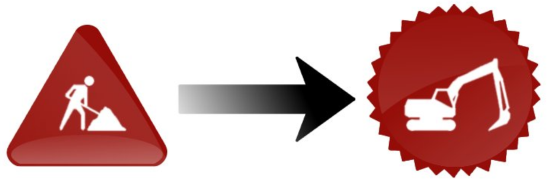
RefactorErl project

- Academic project @ ELTE and ELTE-Soft
  - Researchers, PhD students
  - BSc/MSc student
- Static source code analysis project
- Ananlyses & transformations
- plc.inf.elte.hu/erlang

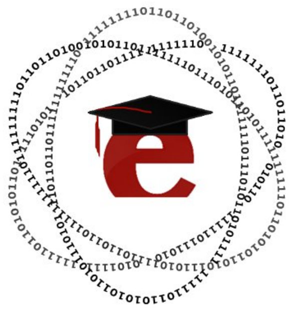
NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Static analysis framework

Effective software maintenance



- Understand legacy code
- Refactoring/Application restructuring
- Code checking: complexity/**quality**/style/**vulnerability**/custom properties



Knowledge sharing

in Erlang

for Erlang

National Research, Development and Innovation Office Hungary

PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

National Research, Development and Innovation Office
Hungary
PROGRAM FINANCED FROM THE NRDI FUND

RefactorErl-Wombat Workshop

- Cooperation with the innovation management team
- November 2022
- WombatOAM by Erlang Solutions
  - Operations & Maintenance Tool
  - Monitoring - metrics, alarms, logs
  - Orchestration - deploying nodes
- How can SA help to find the source of the alarms?
  - memory overload
  - orphan processes
- How can DA help to make SA more accurate?
- The discussion turned the attention to Security Auditing
  - Vulnerability checkers by RefactorErl

12:50 – 13:00	Welcome
13:00 – 13:15	**Dániel Horpácsi.** R&D&I in the RefactorErl-Wombat synergy
13:15 – 13:30	**Melinda Tóth.** Static analysis in Erlang
13:30 – 13:45	**Mohamed Ali Khechine.** Dynamic analysis in Erlang
13:45 – 14:00	**Róbert Fikó.** First steps of the fusion
14:00 – 15:00	Discussion
15:00 –	Finger food

National Research, Development and Innovation Office
Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the “esg” layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding “error-path” based on symbolic execution
- Coverage-based test case generation
- Spec generation

National Research, Development and Innovation Office Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Analysing Wombat

- Found 85 vulnerabilities (63 sec)
- 3 old crypto calls
- 22 injection
  - port creation (2), os call (14), compile operation (6)
- 1 prioritisation
- 59 atom exhaustion
  - unsafe file operation (1), atom creation (58: 13 - 5- 40) Security analysis of industrial partner's code

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the “esg” layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade

- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding “error-path” based on symbolic execution
- Coverage-based test case generation
- Spec generation

National Research, Development and Innovation Office Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Changing the analyser framework

- Supporting both quick and deep/accurate/slow analysis as well
- Multi-layer framework
- Simplifying the analyser backend
- Removed "esg" and parallelism
  - reduced execution time: >30%
  - the final result is not consistent
  - the synchronisation server needs to be removed
- In memory not yet tested

National Research, Development and Innovation Office Hungary
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade

- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the "esg" layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade

- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding "error-path" based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Topics — August, 2022 - January, 2023

- Security analysis of industrial partner's code
  - improvements on the checkers
    - bugfixes
    - false positive elimination
    - false negative reduction
  - prioritisation
  - analysing the results
- Static and dynamic analysis fusion
- Simplifying the analyser framework
  - removing the “esg” layer
  - in memory analysis
- Green Computing
- Supporting safe code upgrade
- Improving data-flow analysis
- Scriptable UI
- Impact analyser improvements
- Analysing distributed Erlang applications
- Extending/improving the security analysis
- Rebar3 build
- Supporting first-time users: docker and public web service
- Finding concurrent design pattern candidates
- Finding “error-path” based on symbolic execution
- Coverage-based test case generation
- Spec generation

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

Project in numbers

- Members
  - 2 researchers
  - 2 PhD students (+1 ?)
  - 10 + 15 MSc students
  - 2 BSC students

- 1 conference paper appeared
- 1 journal paper accepted
- 1 journal paper submitted (under revision)

- 3 minor revision requested
- 3 major revision requested
- 2 under review

- 5 ongoing MSc theses (May 2023)
- 1 BSc thesis (Jan. 2023), 1 ongoing (May 2023)
- 1 MSc thesis (Univ. Novi Sad)
- Industrial connection
  - Erlang Solutions
  - Ericsson
  - OTP
- ErlangOTP Training in November
  - OTP - November
- International cooperation
  - Univ. Novi Sad, 1 paper under revision, 1 MSc thesis defended
- International project involvement
  - COST CA19135 - CERCIRAS

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE HUNGARY
PROGRAM FINANCED FROM THE NRDI FUND

THANK YOU FOR YOUR ATTENTION

Application Domain Specific Highly Reliable IT Solutions project has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme.

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM FINANCED FROM THE NRDI FUND