STATIC ANALYSIS OF ERLANG PROGRAMS

ISTVÁN BOZÓ, MELINDA TÓTH

REFACTORERL PROJECT

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

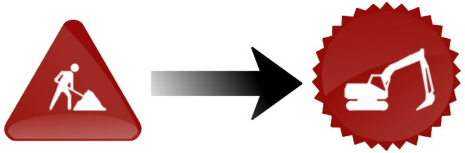
National Research, Development and Innovation Office
Hungary

PROGRAM
FINANCED FROM
THE NRDI FUND

Key benefits

- Shorten **learning term** of a newcomer
- Shorten **bug** report solution time
- Make the possibility of a better team work
- Support software delivery product line
- Increase code quality by reducing faults
- **Shorten time-consuming daily jobs**
- Helps to detect **vulnerabilities** and undesired software properties

Effective software maintenance



NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

Main features

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

Knowledge sharing

National Research, Development and Innovation Office
Hungary

PROGRAM
FINANCED FROM
THE NRDI FUND

Static analysis framework

- Compile-time analysis
- Functions, variables, records, etc
- Lifetime, scope, visibility
- Static and dynamic references
- Side-effects
- Data-flow, control-flow
- Dynamic function call graph
- Hidden dependencies

in Erlang

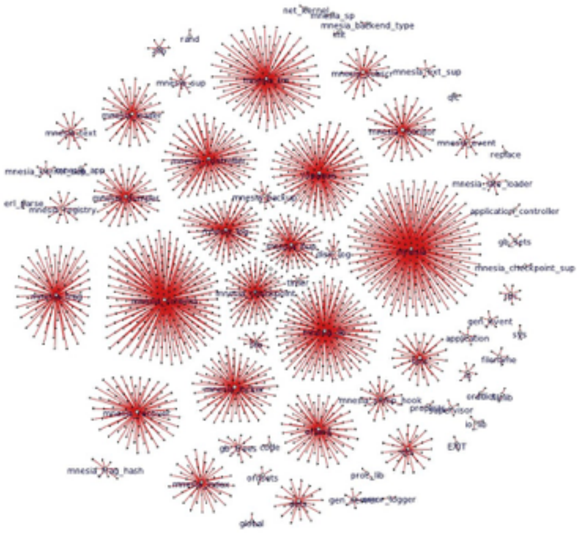
for Erlang

National Research, Development and Innovation Office
Hungary

PROGRAM
FINANCED FROM
THE NRDI FUND

Program development support through

- Semantic queries
- Software complexity metrics
- Bad smell detection
- Duplicated code detection and elimination
- Clustering - software restructuring
- Dependency visualisation
- Secure programming
- Code quality checking

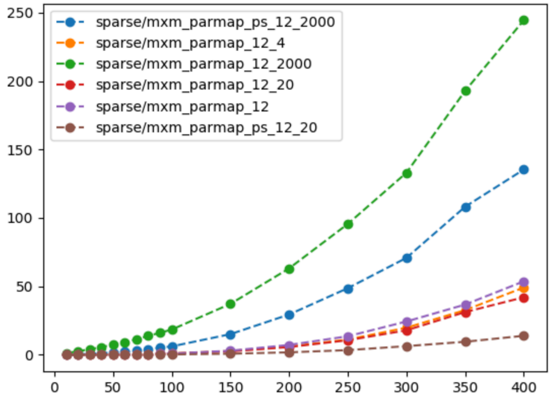


National Research, Development and Innovation Office
Hungary

PROGRAM
FINANCED FROM
THE NRDI FUND

And lots of experiments on

- Communication/process relation analyses
- Program slicing for test case selection
- OTP behaviour analyses
- Decompilation
- Pattern candidate discovery and refactorings for parallelisation
- Ad-hoc parellelisation
- Distribution analysis and refactorings to introduce distribution
- Improving the “functional style” of the code
- Merging static and dynamic analyses
- Green computing



NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

TKP topics in 2019-2022

- Checking various software properties
  - Support for secure coding
  - Design rule classification
  - Complexity metrics
- Automatised rule checking based on configurations
- Analysing distributed Erlang applications
- Improving data-flow analysis
- Erlang LS integration / VSCode interface
- Supporting first-time users
- BEAM analysis
- Elixir analysis
- Support for software/service migration
- Finding concurrent design pattern candidates
- Finding “error-path” based on symbolic execution
- Distributed database backend
- Refactoring concurrent Erlang applications for distribution
- Refactorings for optimising functional code
- Graph-based duplicated code analysis
- Software dependency visualisation to support code comprehension
- Model for storing software versions
- Analysing the fingerprint of the programmers
- Green Computing
- Fixes and improvements on RefactorErl

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

TKP in numbers

- Members
  - 2 researchers
  - 2+3 PhD students
  - ca 40 MSc students
  - ca 10 BSC students
- 3 + 13 Journal papers
- 7 Conference papers
- 10 Abstracts
- 17 Conference talks
- 4 invited talks

- 11 TDK theses
- 9 presented OTDK theses
  - 7 prizes
- 14 Master theses
- 10 Bachelor theses
- 2 Internships
- Industrial connection
  - Ericsson
  - OTP
- Trainings
  - OTP
- International cooperation
  - Univ. Novi Sad, SSQSA
- International project involvment
  - COST CA19135 - CERCIRAS

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

Checking software properties

- Coding convention
- Design rules
- Style
- Complexity
- Custom properties
- Non-intentional software **vulnerabilities**

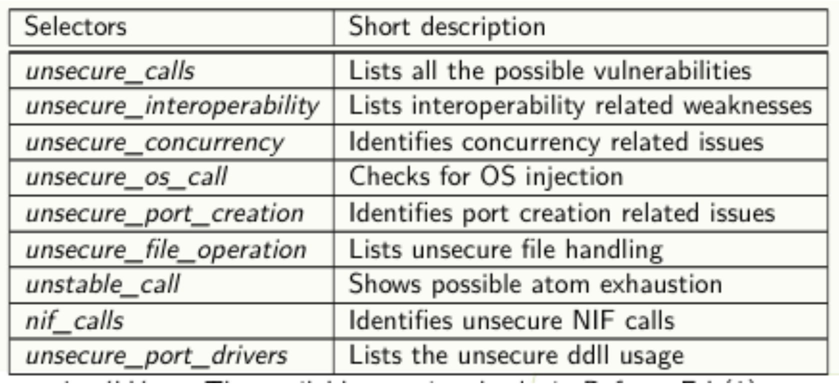
clause-limit
exported-functions-limit
exported-without-spec
used-underlined-var
find-function-call
find-io-format
no-imports
tag-messages
flush-message-box
tail-recursive-servers
macro-naming
no-nested-try-catch
module-naming
function-naming
state-for-otp-behaviours
etc...

National Research, Development and Innovation Office
Hungary

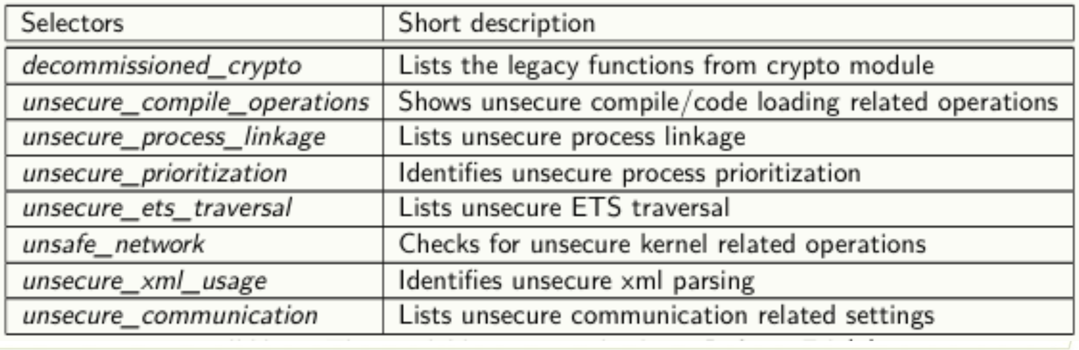
PROGRAM
FINANCED FROM
THE NRDI FUND

Vulnerability checks

- Support for secure coding
- Erlang specific analysis
- Identify unsecure function calls and constructs
- Filter those based on data-flow analysis (taint analysis)



Selectors	Short description
unsecure_calls	Lists all the possible vulnerabilities
unsecure_interoperability	Lists interoperability related weaknesses
unsecure_concurrency	Identifies concurrency related issues
unsecure_os_call	Checks for OS injection
unsecure_port_creation	Identifies port creation related issues
unsecure_file_operation	Lists unsecure file handling
unstable_call	Shows possible atom exhaustion
nif_calls	Identifies unsecure NIF calls
unsecure_port_drivers	Lists the unsecure ddll usage



Selectors	Short description
decommissioned_crypto	Lists the legacy functions from crypto module
unsecure_compile_operations	Shows unsecure compile/code loading related operations
unsecure_process_linkage	Lists unsecure process linkage
unsecure_prioritization	Identifies unsecure process prioritization
unsecure_ets_traversal	Lists unsecure ETS traversal
unsafe_network	Checks for unsecure kernel related operations
unsecure_xml_usage	Identifies unsecure xml parsing
unsecure_communication	Lists unsecure communication related settings

NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
HUNGARY

PROGRAM
FINANCED FROM
THE NRDI FUND

Vulnerability checks

- Support for secure coding
- **Erlang specific analysis**
- Identify unsecure function calls and constructs
- Filter those based on data-flow analysis (taint analysis)

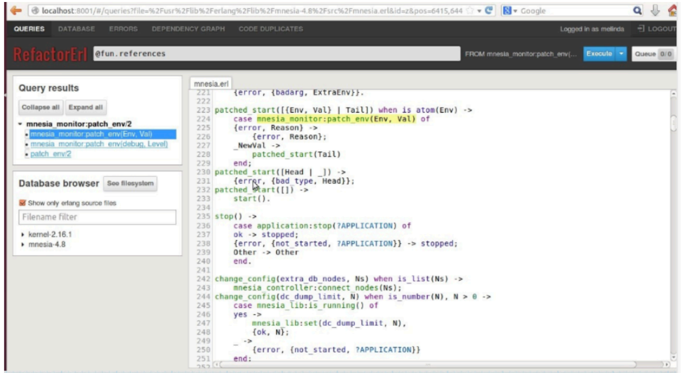
- Injection
- Memory overload
- Interoperability mechanism related issues
- Concurrent/distributed programming related issues

National Research, Development and Innovation Office
Hungary

PROGRAM
FINANCED FROM
THE NRDI FUND

Code Checking

- Semantic Query Language
- Standalone, automatic rule checker interface: DRC
- Diagnostics in ELS


localhost:8001/#/queries?file=%2Fusr%2Flib%2Ferlang%2Flib%2Fmnesia-4.8%2Fsrc%2Fmnesia.erl&id=z&pos=6415,644
Google
QUERIES
DATABASE
ERRORS
DEPENDENCY GRAPH
CODE DUPLICATES
Logged in as melinda
LOGOUT
RefactorErl
FROM mnesia_monitor:patch_env(...
Execute
Queue 0/0
Query results
Collapse all
Expand all
mnesia_monitor:patch_env/2
mnesia_monitor:patch_env(Env, Val)
mnesia_monitor:patch_env(debug, Level)
patch_env/2
Database browser
See filesystem
Show only erlang source files
Filename filter
kernel-2.16.1
mnesia-4.8
mnesia.erl

```
@fun.references
```

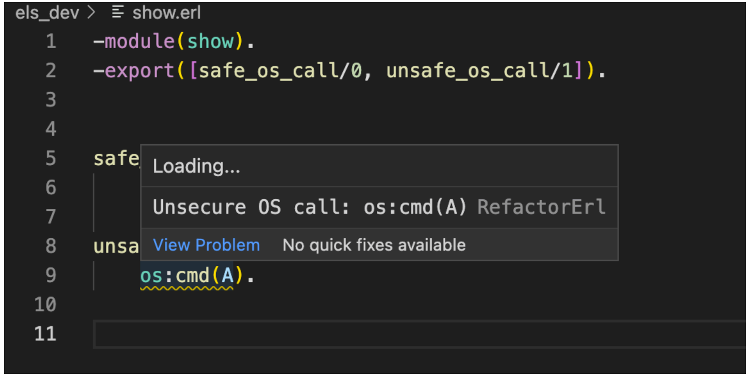
```
    {error, {badarg, ExtraEnv}}.

patched_start([{Env, Val} | Tail]) when is atom(Env) ->
    case mnesia_monitor:patch_env(Env, Val) of
    {error, Reason} ->
        {error, Reason};
    _NewVal ->
        patched_start(Tail)
    end;
patched_start([Head | _]) ->
    {error, {bad_type, Head}};
patched_start([]) ->
    start().

stop() ->
    case application:stop(?APPLICATION) of
    ok -> stopped;
    {error, {not_started, ?APPLICATION}} -> stopped;
    Other -> Other
    end.

change_config(extra_db_nodes, Ns) when is_list(Ns) ->
    mnesia_controller:connect_nodes(Ns);
change_config(dc_dump_limit, N) when is_number(N), N > 0 ->
    case mnesia_lib:is_running() of
    yes ->
        mnesia_lib:set(dc_dump_limit, N),
        {ok, N};
    _ ->
        {error, {not_started, ?APPLICATION}}
    end;
```

mods.funs.unsecure_prioritization



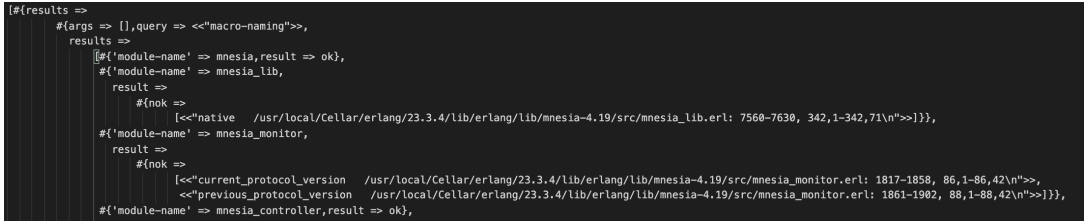
```
-module(show).
-export([safe_os_call/0, unsafe_os_call/1]).


safe
 
 
unsa
    os:cmd(A).
```

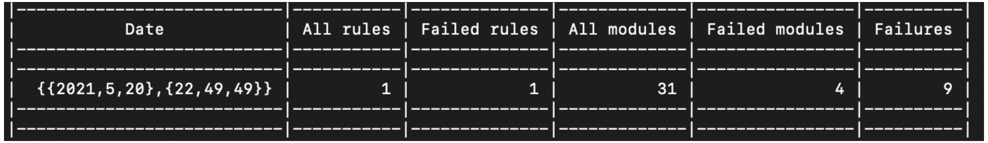
Loading...

Unsecure OS call: os:cmd(A) RefactorErl

View Problem   No quick fixes available



```
[#{results =>
       #{args => [],query => <<"macro-naming">>,
         results =>
             [#{'module-name' => mnesia,result => ok},
              #{'module-name' => mnesia_lib,
                result =>
                    #{nok =>
                          [<<"native   /usr/local/Cellar/erlang/23.3.4/lib/erlang/lib/mnesia-4.19/src/mnesia_lib.erl: 7560-7630, 342,1-342,71\n">>]}},
              #{'module-name' => mnesia_monitor,
                result =>
                    #{nok =>
                          [<<"current_protocol_version   /usr/local/Cellar/erlang/23.3.4/lib/erlang/lib/mnesia-4.19/src/mnesia_monitor.erl: 1817-1858, 86,1-86,42\n">>,
                           <<"previous_protocol_version   /usr/local/Cellar/erlang/23.3.4/lib/erlang/lib/mnesia-4.19/src/mnesia_monitor.erl: 1861-1902, 88,1-88,42\n">>]}},
              #{'module-name' => mnesia_controller,result => ok},
```



```
|--------------------------|-----------|--------------|-------------|----------------|----------|
|           Date           | All rules | Failed rules | All modules | Failed modules | Failures |
|--------------------------|-----------|--------------|-------------|----------------|----------|
|--------------------------|-----------|--------------|-------------|----------------|----------|
|  {{2021,5,20},{22,49,49}} |         1 |            1 |          31 |              4 |        9 |
|--------------------------|-----------|--------------|-------------|----------------|----------|
|--------------------------|-----------|--------------|-------------|----------------|----------|
```

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