Yearly team meeting!!!

Benoît Bertholon[1]

[1] Security and Trust (SnT) interdisciplinary center, University of Luxembourg, Luxembourg

PhD advisors: Prof. Dr. Pascal Bouvry & Dr. Sebastien Varrette

Fonds National de la
Recherche Luxembourg

Supported by the Fonds National de la Recherche, Luxembourg

Summary

Summary

3^{rd} year of PhD

Studies

- 2005-2008: Engineer Degree (ISEP Paris).
- 2007-2009: Master Degree "Secure and Dependable Computer System" (Chalmers, Sweden).
- 2009: Master Thesis, (Uni, Luxembourg).

PhD

- 2010-2012 (13?): PhD Confidentiality and Integrity Issues over Cloud Computing Platforms (Uni, Luxembourg).

Summary

CertiCloud Framework

CertiCloud: Framework for IaaS Cloud platforms

- Dedicated to increase security of IaaS platforms
- Based on Trusted Computing and TPMs

Worked With

- TPMs.
- Security Protocols.
- X509 Certificats.
- Cloud frameworks: Nimbus, Eucaliptus.

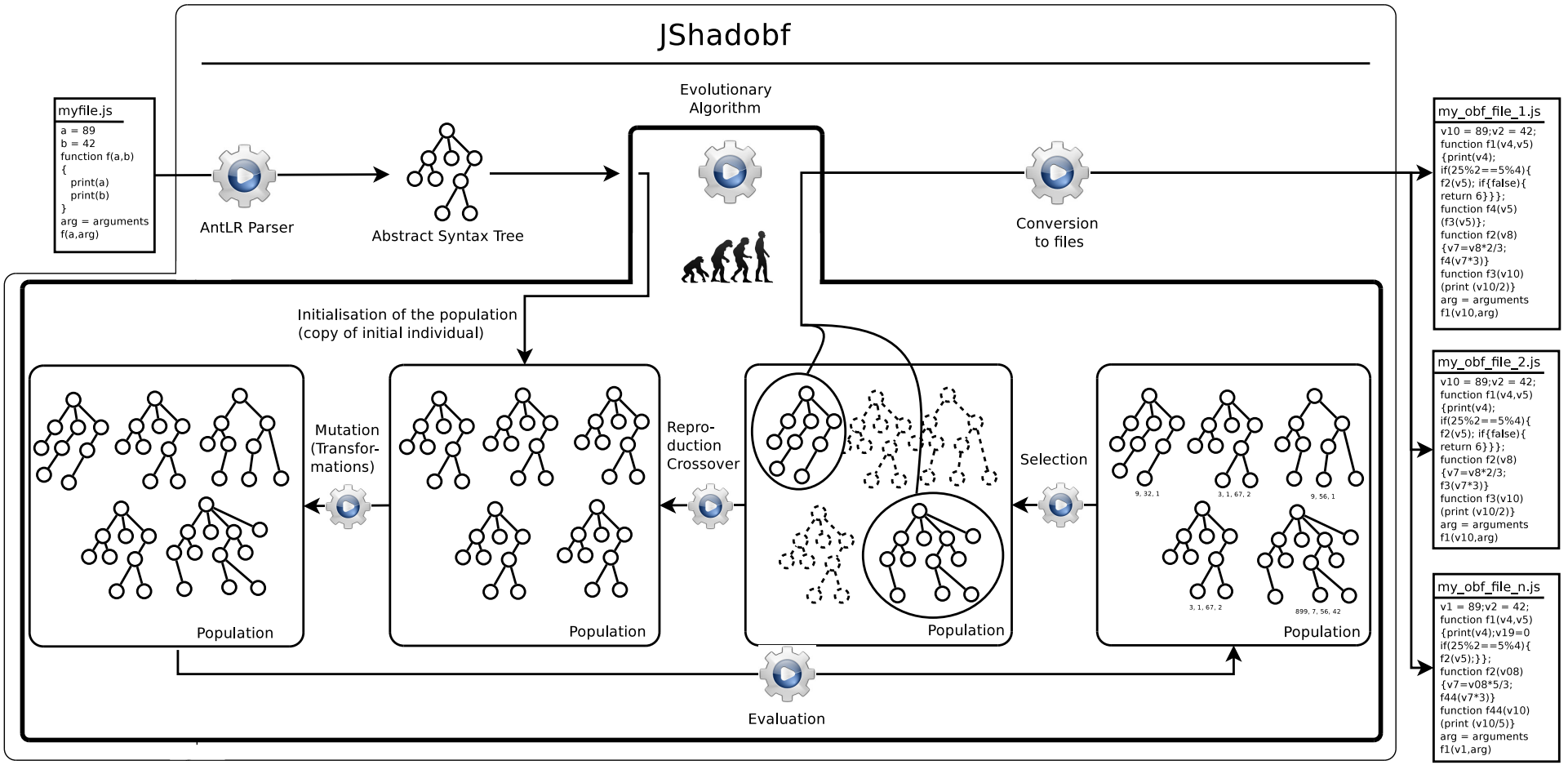
Summary

Problem

Too easy to understand

```
1  function fibo(n)
2  {
3    if( n <= 1 )
4    {
5      return n;
6    }
7    var res = fibo(n-1) + fibo(n-2);
8    return res;
9  }
10 n = parseFloat(arguments[1])
11 nn = fibo(n)
12 print(nn)
```

The Big Picture



Parsing

AntLR

- ANother Tool for Language Recognition.
- Top-Down Parser.

Donwsides

- Parser type: LL(k), less expressive than LR parser.

Advantages

- Python code generation.
- Generation of AST from grammar.
- Active project, lots of existing grammars.
- Possibility of the absence of code in the grammar file.

Transformations

Already implemented

- Renaming.
- Outlining.
- Dummy If insertion.
- Dummy variable insertion.
- Dummy expression insertion.
- Changing place of variable declaration.
- Re-formating string constants.

All ideas are Welcome!!!

Metrics

Metrics

1. Program Length: number of operators & operands in P[Halstead77].
2. Cyclomatic Complexity: number of predicates in F [McCabe76] .
3. Nesting Complexity: nesting level of conditionals in F [Harrison81] .
4. Data Flow Complexity: number of inter-basic block variable references in P [Oviedo80] .
5. Fan-in/out Complexity: number of formal parameters to F, and number of global data structures read or updated by F [Henry81] .

All ideas are Welcome!!!

Crossover

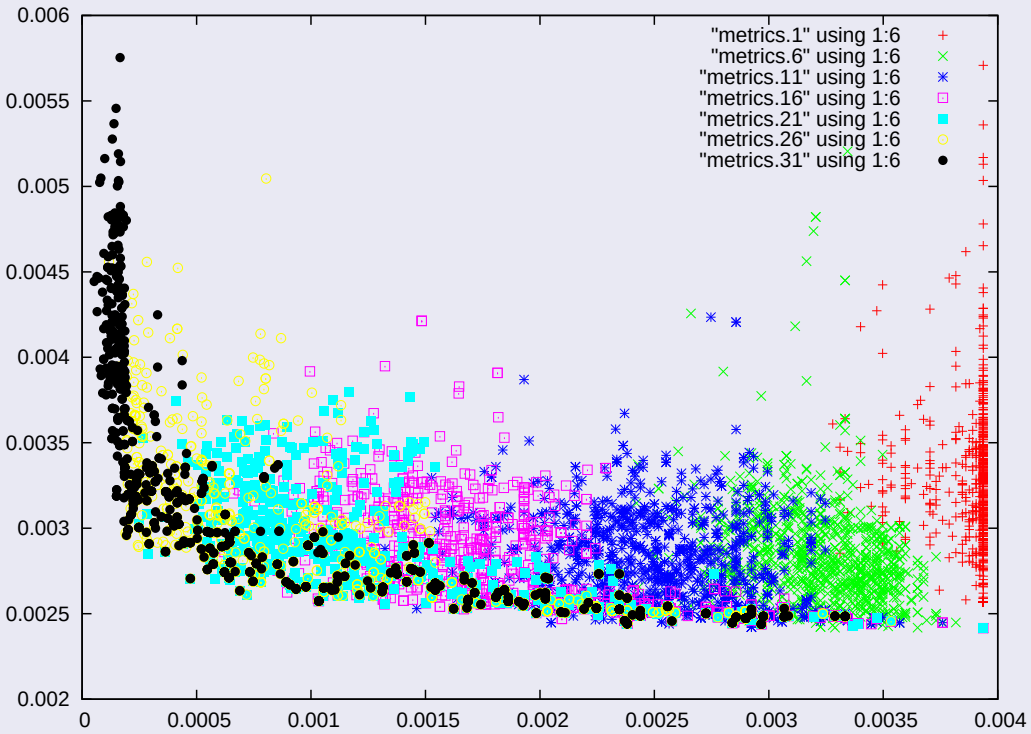
Crossover

- Crossover at the level of functions.
- Problem with outlining.

All ideas are Welcome!!!

Some results with Evolutionary Algorithm

MatMul popsize:1000, generation:31, Length/Time



For Now

Less easy to understand (fibo 100ind, 10 gen, 7min)

```
function a280 (a316) {if((a316 <= 1)){return a316;if((8 > - 2)){;if((- 10 >= -
    10)){;} else {;}} else {if((- 3 < 9)){if((- 7 < 1)){;} else {;};} else {;}-
     1428;;}}if((0 > - 6)){if((- 7 >= 2)){if((- 5 >= 10)){;} else {;};} else {
    var dummyvar680;if((- 10 == - 3)){;} else {;var a31;}};if((- 1 > 0)){if((8
    != 2)){true;;} else {;}var dummyvar258;} else {var dummyvar106;}} else {if
    ((- 3 < 3)){;} else {;};var dummyvar1164;if((0 > 3)){if((- 5 != 3)){;var
    dummyvar374;} else {;};} else {if((- 4 < 3)){;} else {[-
    1261.39774499,6462.65601576,"fkhjsivo wietwsou zqwbkvop igcgtczv zsozrmte
    llwbivvr",false,"bcvhuufj kklzzsad zzvozqey ierncvzr",- 3605.39880946,true,
    true];;};}}var res = (a280((a316  -  1)) + a280((a316  -  2)));return res
    ;}(n = parseFloat(arguments[0]));if((4 <= - 7)){;} else
    {[6427.31361395,6889.57225138,6595.17769932,- 7166];if((- 6 == - 5)){var
    dummyvar1134;} else {;};}if((- 8 <= - 4)){if((1 >= - 8)){;true;if((2 < 1))
    {;"";} else {n;;}} else {;}if((6 >= 1)){if((0 >= 3)){;} else {;};} else {if
    ((2 != - 4)){;} else {;if((0 < - 3)){;} else {;}};if((- 8 != 2)){if((8 < 9)
    ){"bcwwhejp tnkgbzcj quaxtcfs cjelgeug";;} else {;};false;} else {;}};}
    else {;if((- 3 <= 9)){false;;} else {;}}(nn = a280(n));print(nn);
```

Summary

C Obfuscation

Why C?

- Use of PIPS [PIPS].
- PIPS already parse C code.
- PIPS has transformations available.
- PIPS already used with genetic algorithms [GV_Renpar09].

Master Thesis of Sébastien Martinez

- Implementation of Metrics
- Application of Transformations
- Adaptation of genetic algorithms for obfuscation.

Thanks for your attention...

Questions?

email: benoit.bertholon@uni.lu
tel: 00352 466644 5734