A Taint Analysis for the Static Analyzer Goblint

Tutorial at the GobCon 2023

Michael Schwarz Julian Erhard Sarah Tilscher
Helmut Seidl Simmo Saan

{m.schwarz, julian.erhard, sarah.tilscher, helmut.seidl}@tum.de,
simmo.saan@ut.ee

Chair for Formal Languages, Compiler Construction, Software Construction
Department of Informatics, Technical University of Munich

January 2023

Taint Analysis

Question: Can "tainted" information flow somewhere where it's not supposed to go?

- SQL Injection
- Buffer Overflow Attacks
- Key Exfiltration
- . . .

Idea:

- A variable is tainted if it may contain information originating from a *source*
- The analysis should warn if a tainted variable reaches a *sink*

Taint Analysis

Caveat

We are not experts on Taint Analysis, and we will only build a basic analysis today

- No sanitizers
- No implicit flow
- Taints occur at the level of a variable

Additionally, we consider only MiniC, i.e.

- No Multithreading
- (For now) No Pointers

Goblint

Goblint consists of several different components:

- Frontend (offloaded to CIL)
- Abstract Domains
  - Generic: Map, Set, ...
  - Specific to C: BaseDomain, ValueDomain, (Ex/In)clusion Sets, Intervals, . . .
- Analyses
  - Mutex, Threading, Base, . . .
  - In folder `src/analyses/*`
- Fixpoint Solvers

Goblint

Goblint consists of several different components:

- Frontend (offloaded to CIL)
- Abstract Domains
  - Generic: Map, Set, ...
  - Specific to C: BaseDomain, ValueDomain, (Ex/In)clusion Sets, Intervals, . . .
- Analyses
  - Mutex, Threading, Base, . . .
  - In folder `src/analyses/*`
- Fixpoint Solvers

Goblint

Goblint consists of several different components:

- Frontend (offloaded to CIL)
- Abstract Domains
    - Generic: Map, Set, ...
        - In folder `src/domains/*`
    - Specific to C: BaseDomain, ValueDomain, (Ex/In)clusion Sets, Intervals, ...
        - In folder `src/cdomains/*`
- Analyses
    - Mutex, Threading, Base, ...
    - In folder `src/analyses/*`
    - Taint Analysis
- Fixpoint Solvers

Diagram

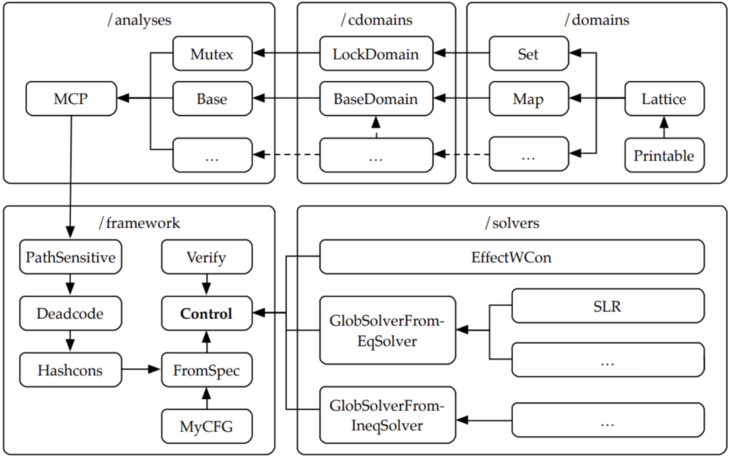

Figure: Architecture of Goblint (from Apinis '14)

First steps

You may jump right in by looking at the file which contains notes on how to get started: `analyses/tutorials/taint.ml`!

We have provided regression tests, which you can run with

```
ruby scripts/update_suite.rb group tutorials
```

Questions?