DAFL:
Directed Grey-box Fuzzing Guided by Data Dependency

Tae Eun Kim, Jaeseung Choi, Kihong Heo, Sang Kil Cha

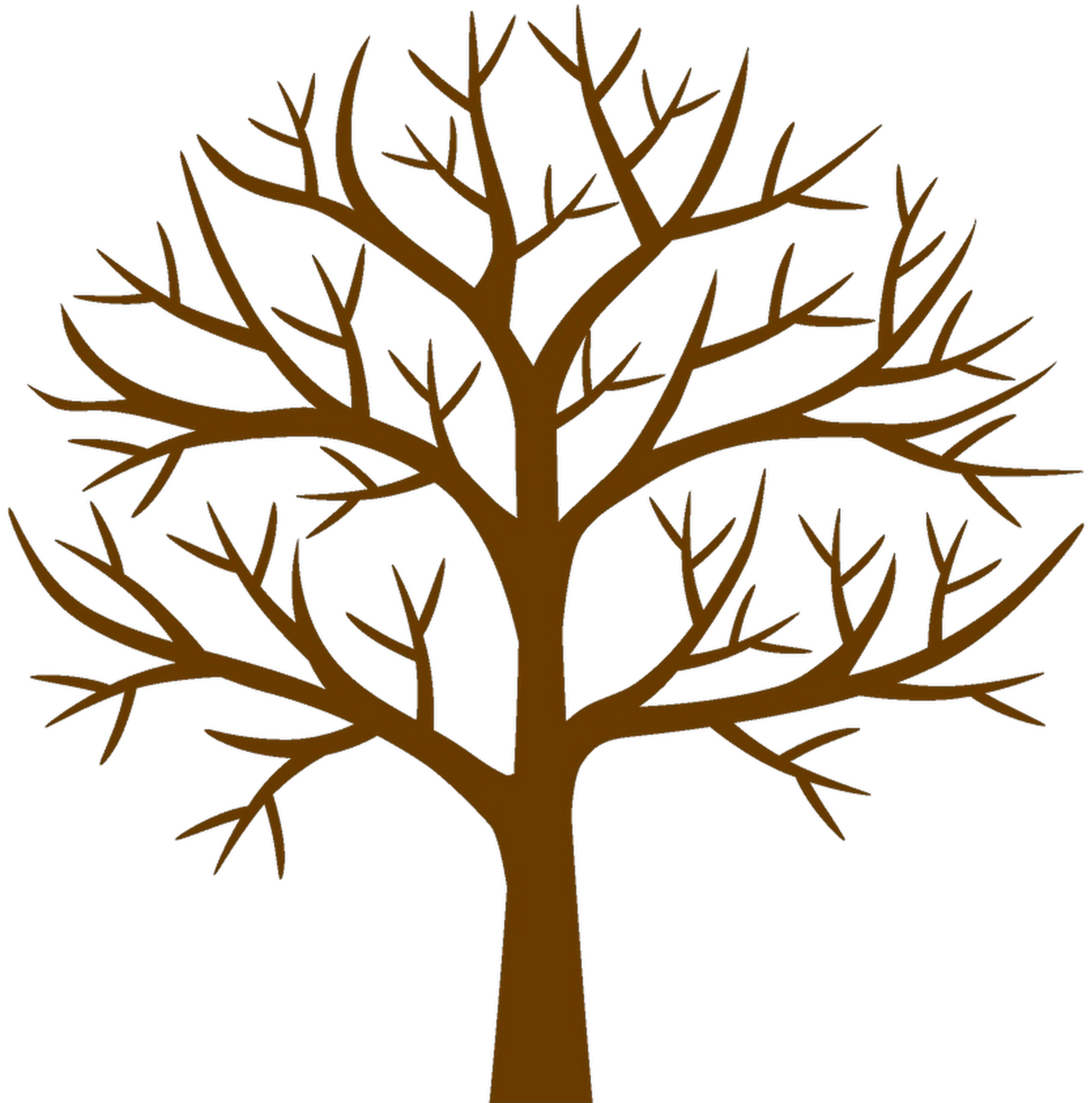
KAIST

SOGANG UNIVERSITY

Background

Fuzzing

- Testing a program with randomly generated inputs
- Successful achievements
  - e.g., AFL, Google’s OSS Fuzz project



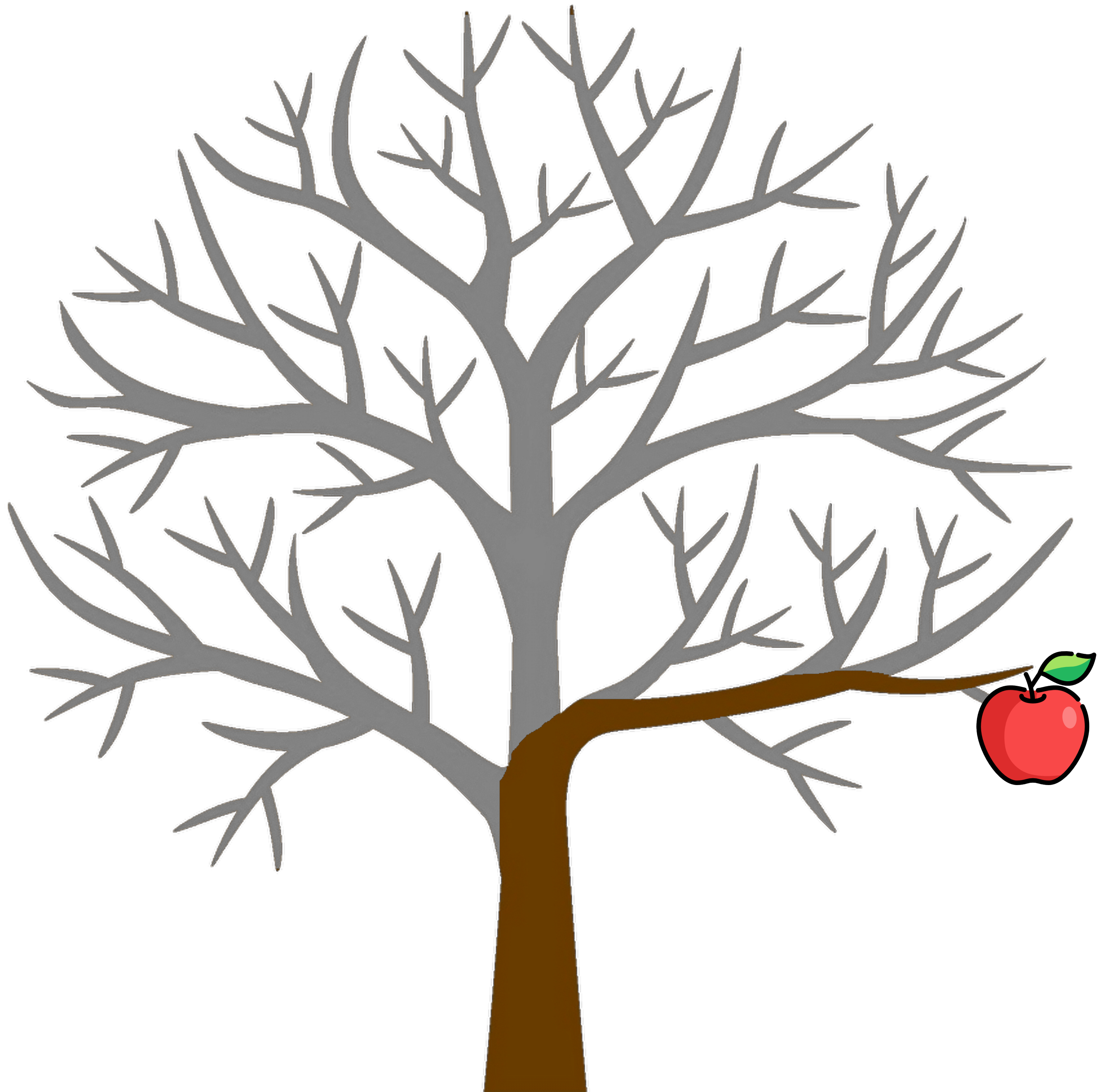
Background

Fuzzing

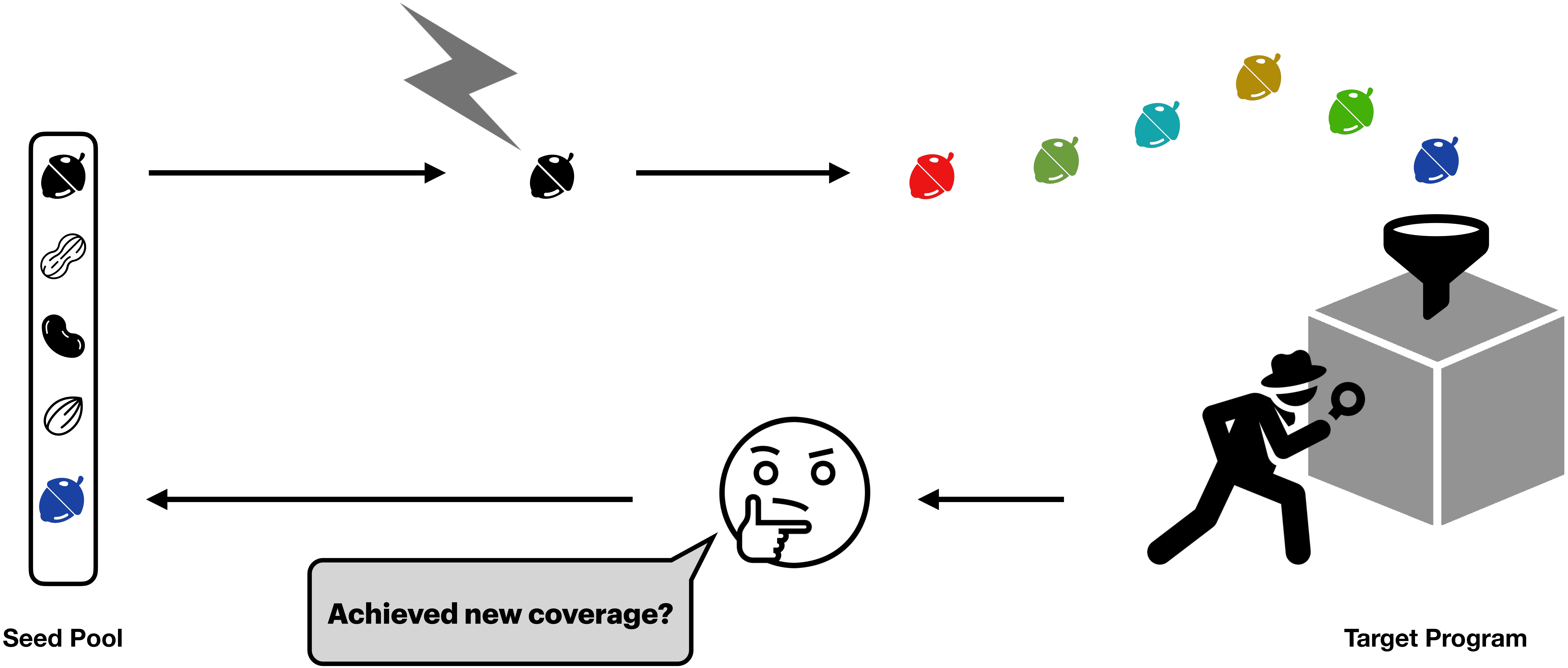
- Testing a program with randomly generated inputs
- Successful achievements
    - e.g., AFL, Google’s OSS Fuzz project

Directed Fuzzing

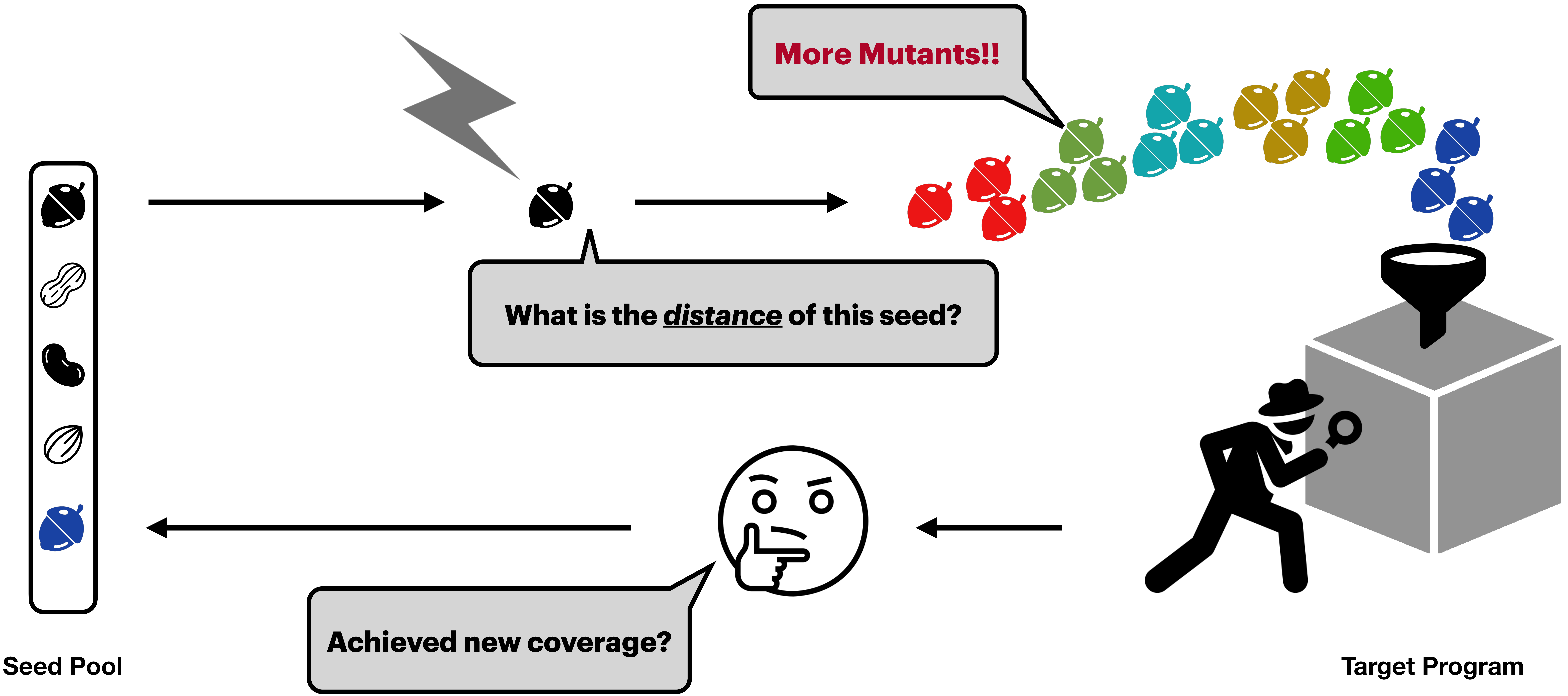
- Aims to reach the given target location(s)
    - Generate crashing inputs from bug reports (e.g., static analysis alarms)



Directed Grey-box Fuzzing (DGF)



Directed Grey-box Fuzzing (DGF)



More Mutants!!

What is the *distance* of this seed?

Achieved new coverage?

Seed Pool

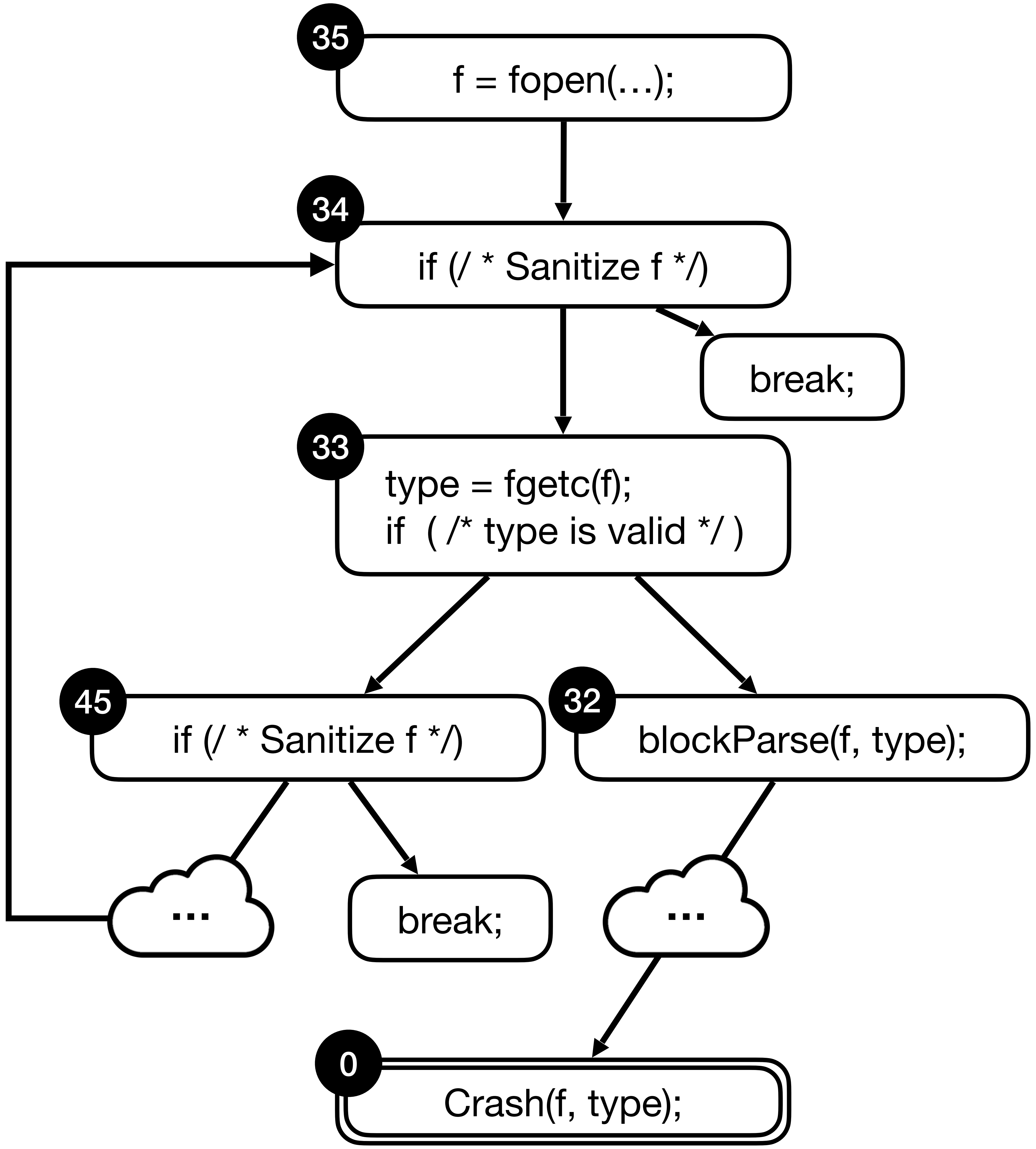
Target Program

Limitations of DGF

1. **Noisy** seed distance based on Control Flow Graph (CFG)
    - Complex control structures (e.g., loops) introduce noise in the seed distance

Limitations of DGF

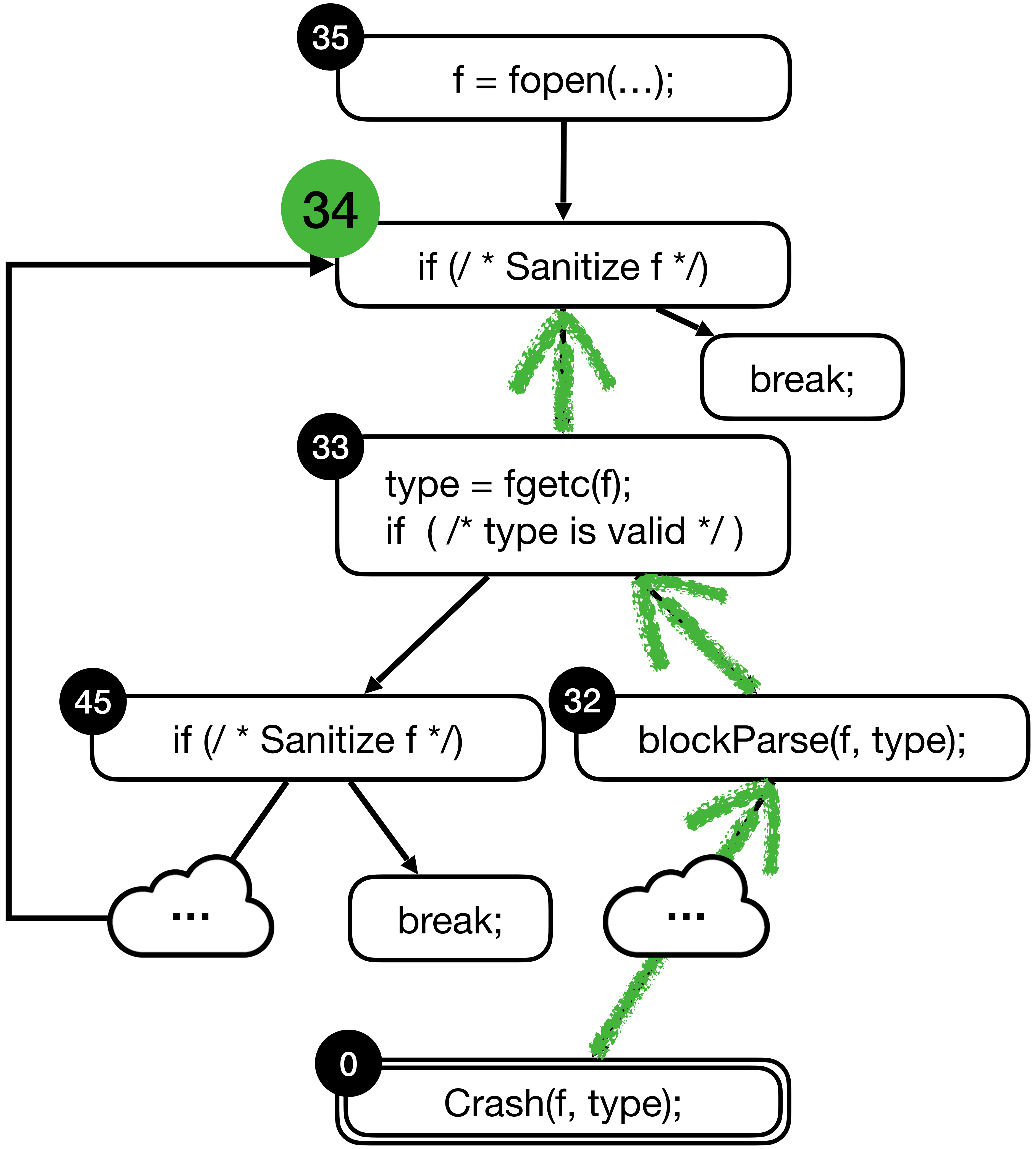
Noisy CFG-based Seed distance



*CVE-2017-7578 in swftophp

Limitations of DGF

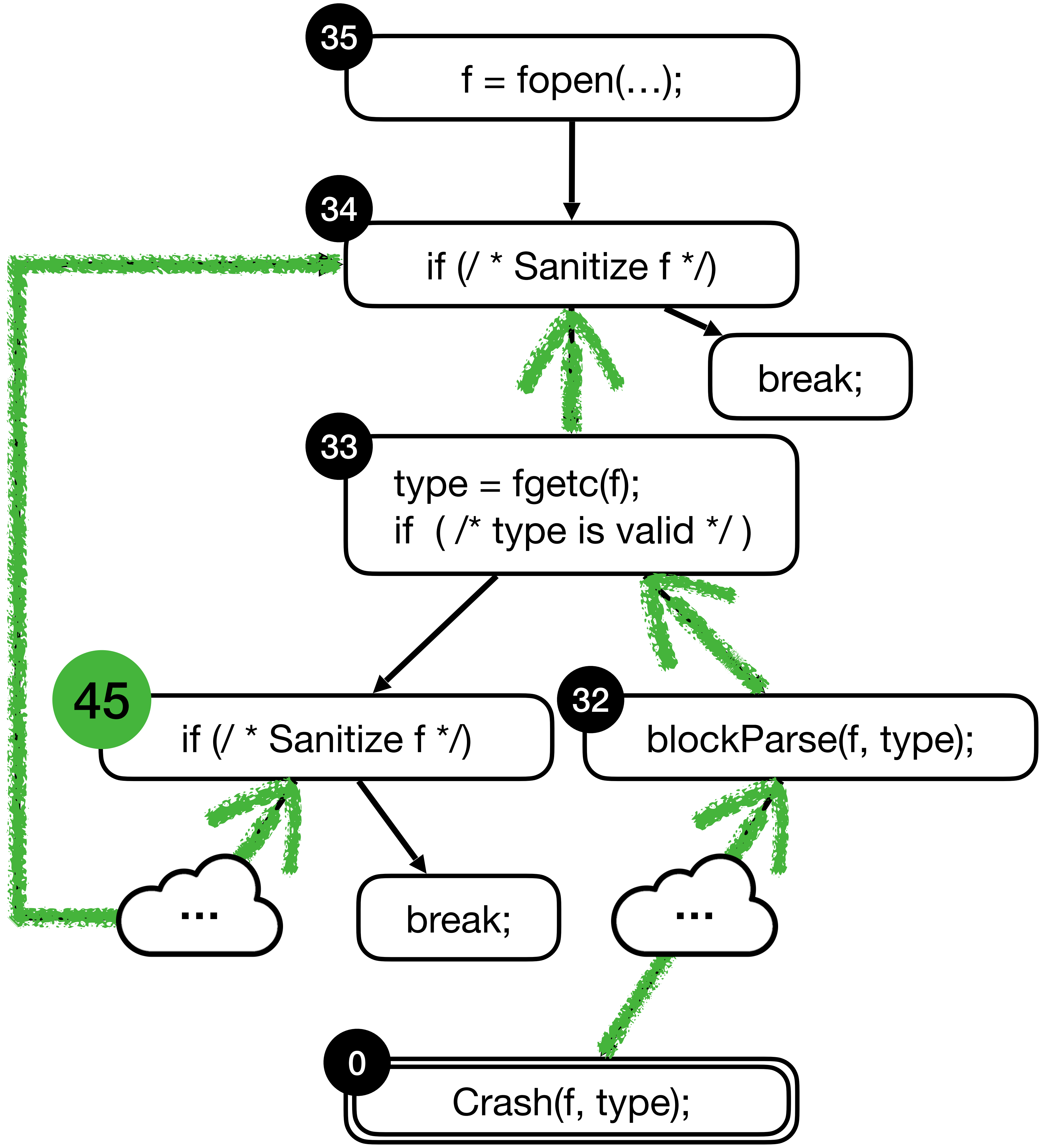
Noisy CFG-based Seed distance



*CVE-2017-7578 in swftophp

Limitations of DGF

Noisy CFG-based Seed distance



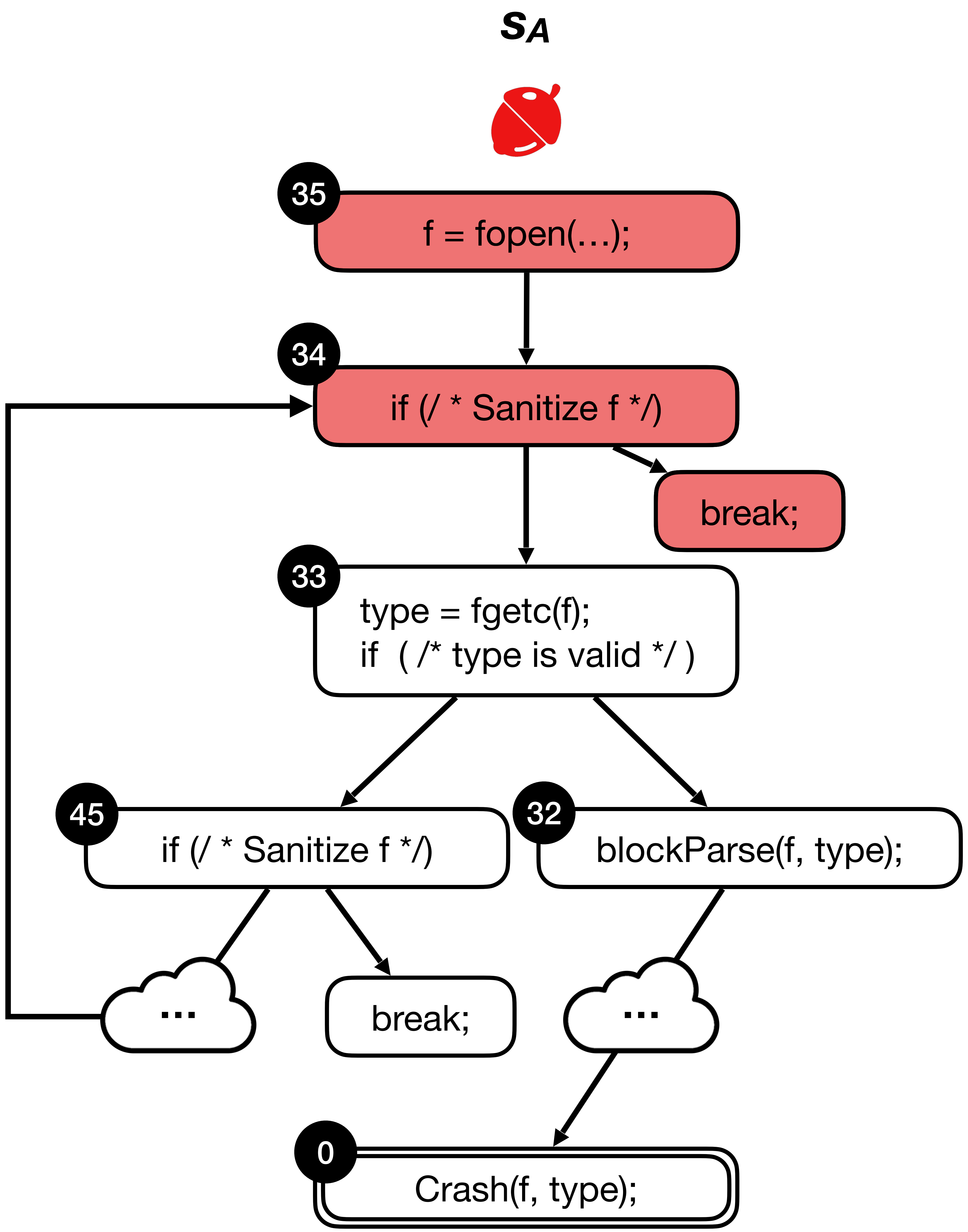
*CVE-2017-7578 in swftophp

Limitations of DGF

Noisy CFG-based Seed distance

AFLGo: Distance based on all nodes in CFG (Lower is Better)

🍎 **34.5** Averge(34, 35)



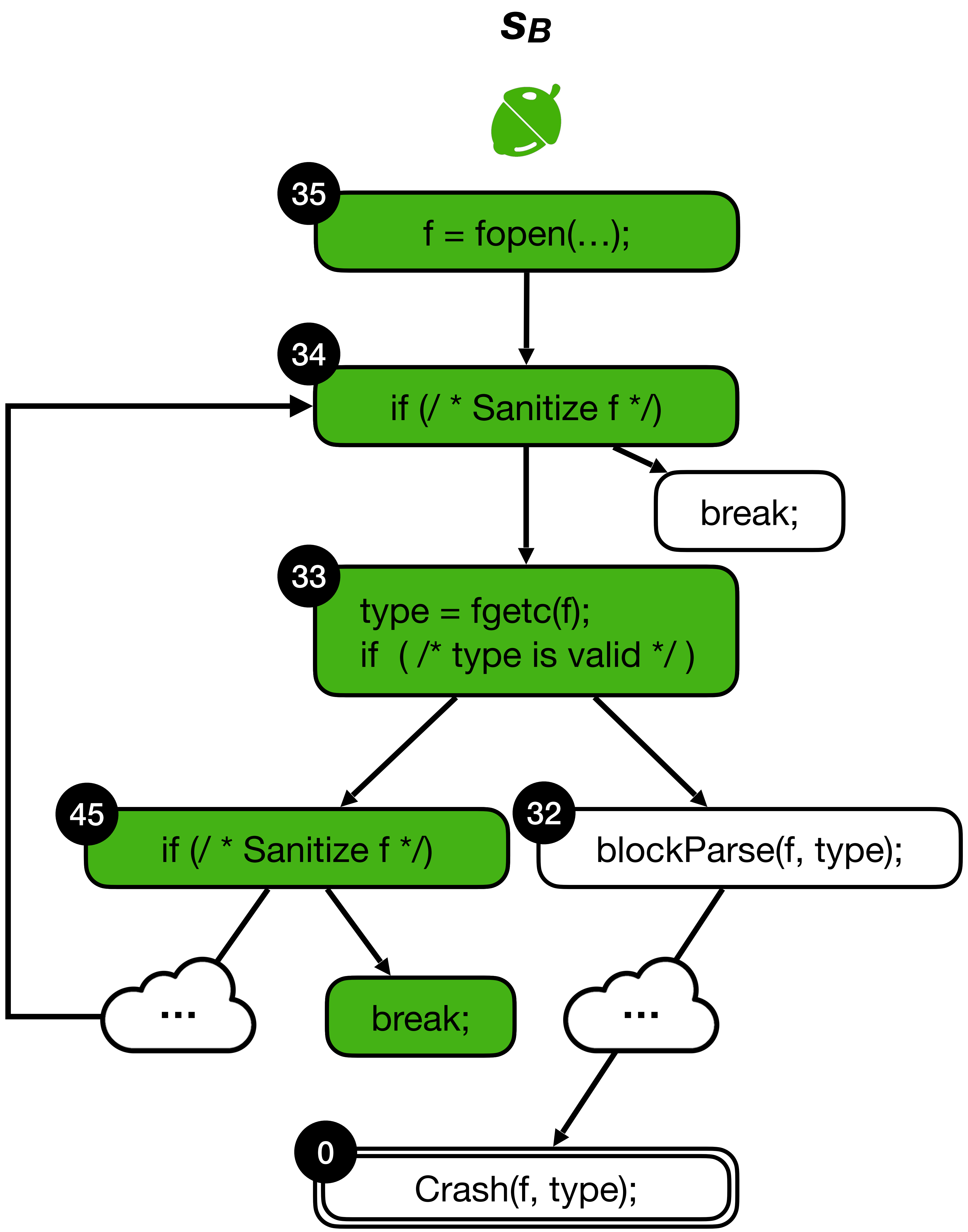
*CVE-2017-7578 in swftophp

Limitations of DGF

Noisy CFG-based Seed distance

AFLGo: Distance based on all nodes in CFG (Lower is Better)

34.5	Averge(34, 35)
37.5	Averge(34, 35, 36, 45)



*CVE-2017-7578 in swftophp

Limitations of DGF

Noisy CFG-based Seed distance

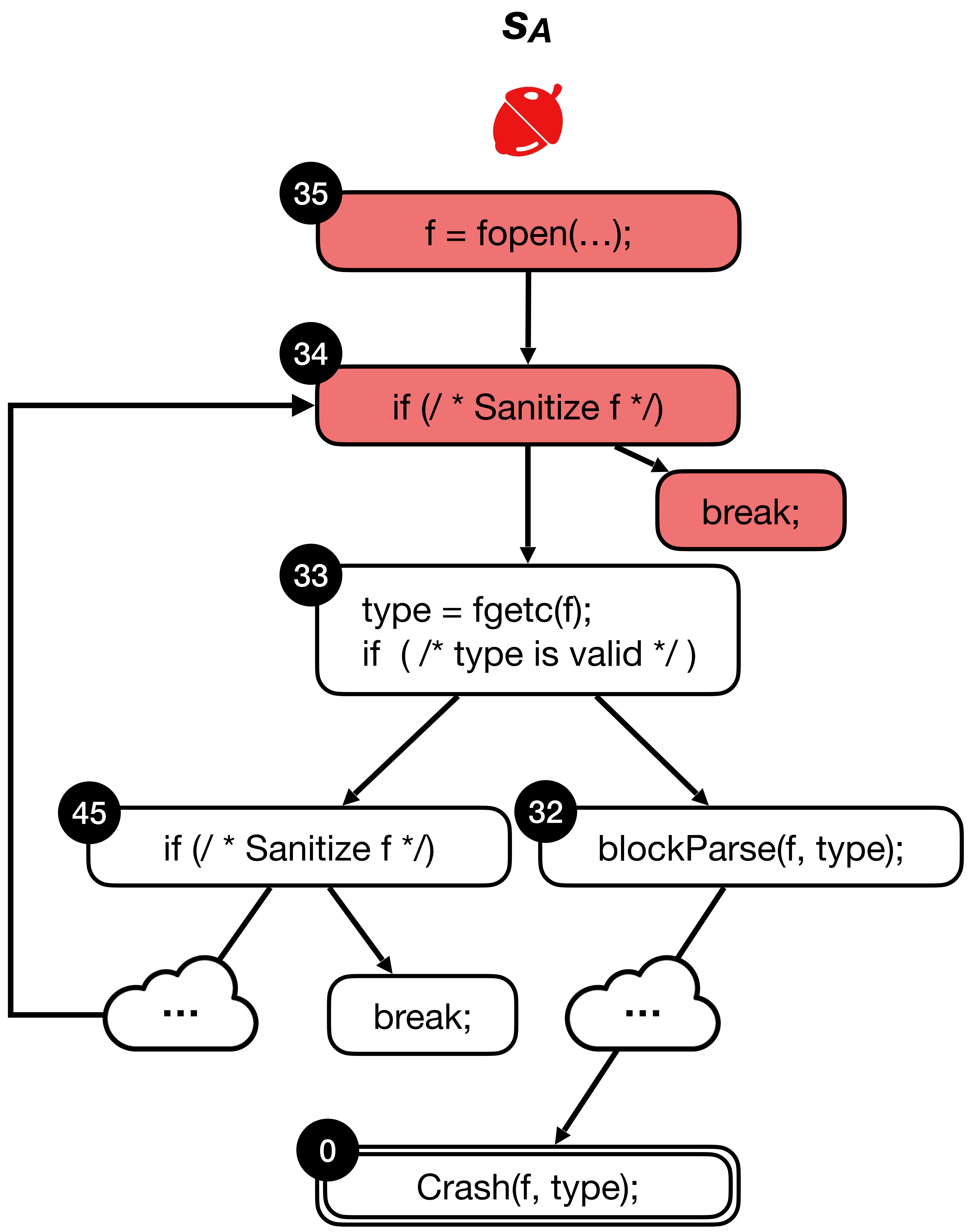
AFLGo: Distance based on all nodes in CFG (Lower is Better)

👍 🔴 **34.5**

🟢 **37.5**

WindRanger: Distance based on Diverging nodes in CFG

🔴 **34** (Lower is Better)



*CVE-2017-7578 in swftophp

Limitations of DGF

Noisy CFG-based Seed distance

AFLGo: Distance based on all nodes in CFG (Lower is Better)

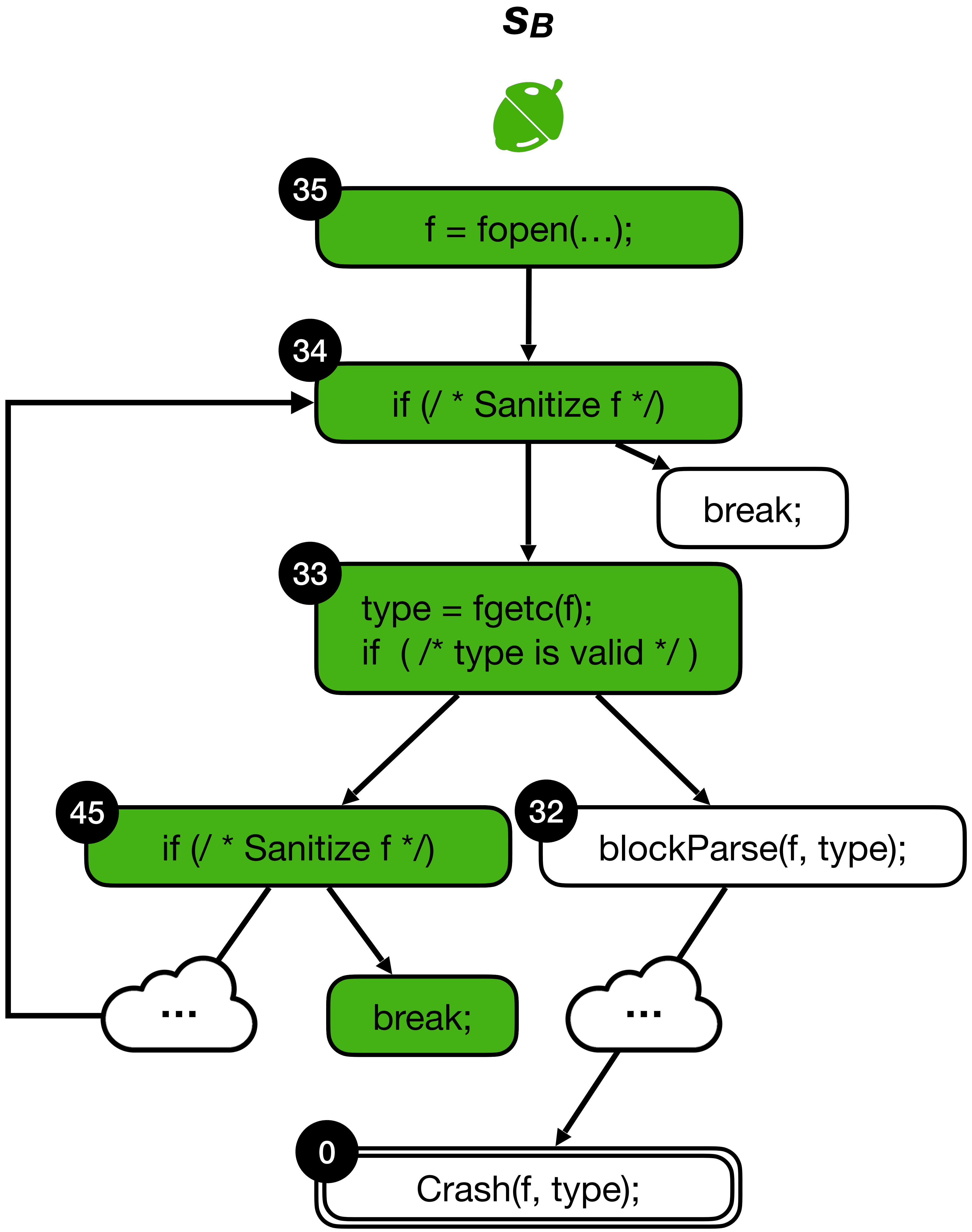
👍 🟥 **34.5**

🟩 **37.5**

WindRanger: Distance based on Diverging nodes in CFG (Lower is Better)

👍 🟥 **34**

🟩 **45**



*CVE-2017-7578 in swftophp

DAFL’s Solution

DUG-based Semantic Relevance Score

AFLGo: Distance based on all nodes in CFG

✓ 34.5 Averge(34, 35)

✗ 37.5 Averge(34, 35, 36, 45)

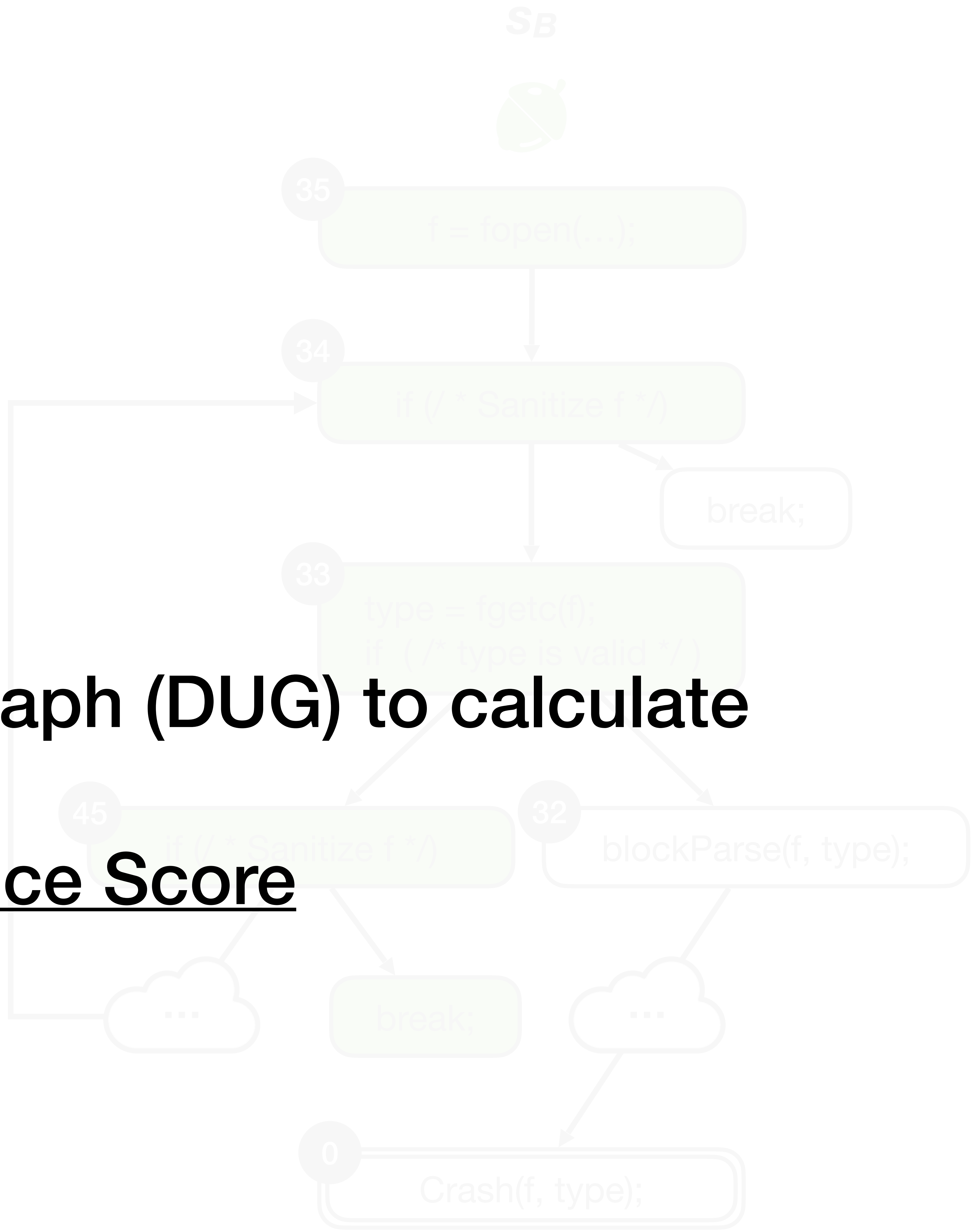
DAFL utilizes Definition-Use Graph (DUG) to calculate

Semantic Relevance Score

WindRanger: Distance based on Diverging nodes in CFG

✓ 34

✗ 45



*CVE-2017-7578 in swftophp

DAFL’s Solution

DUG-based Semantic Relevance Score

AFLGo: Distance based on all nodes in CFG (Lower is Better)

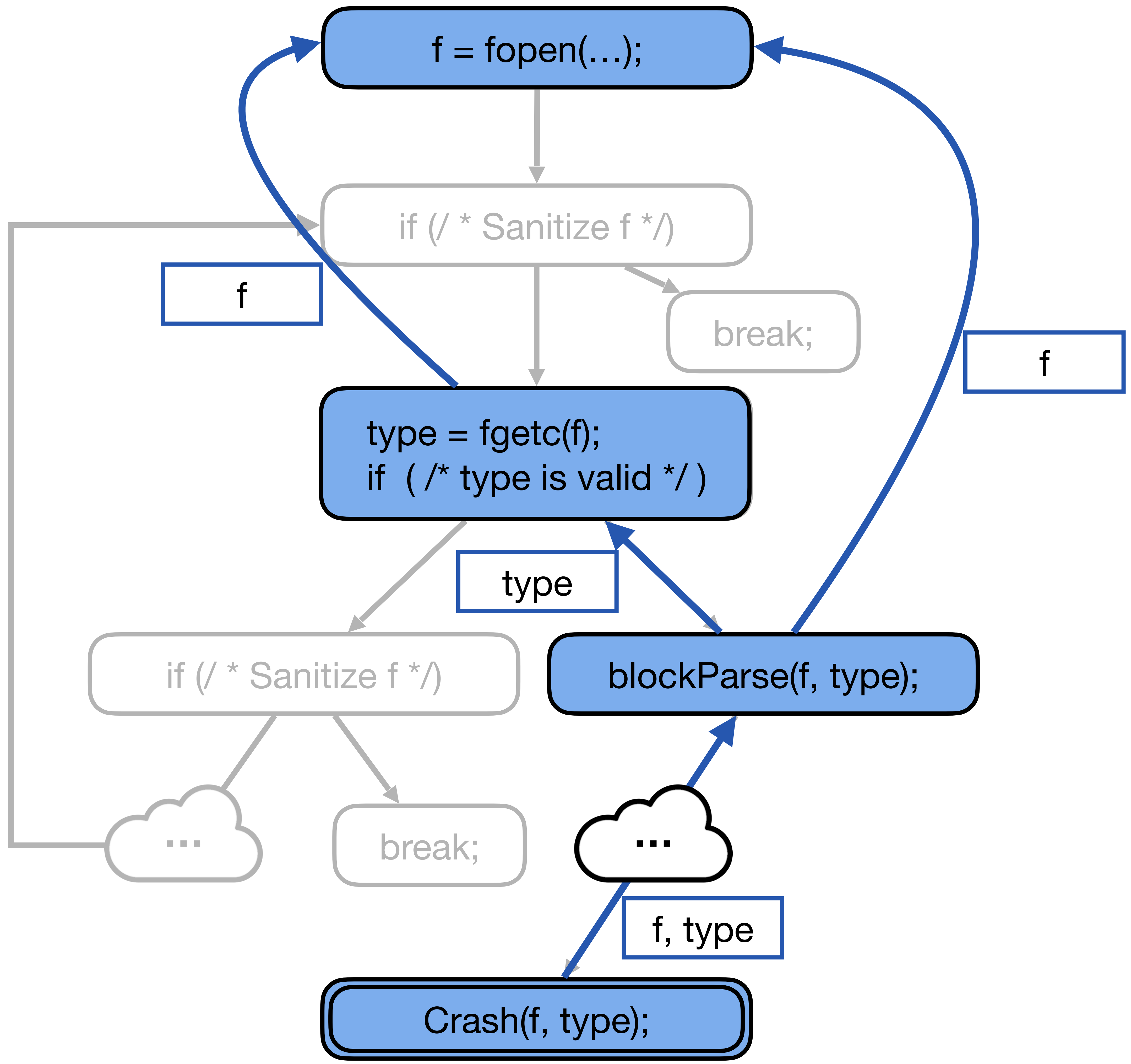
👍 🔴 **34.5**

🟢 **37.5**

WindRanger: Distance based on Diverging nodes in CFG (Lower is Better)

👍 🔴 **34**

🟢 **45**



*CVE-2017-7578 in swftophp

DAFL’s Solution

DUG-based Semantic Relevance Score

AFLGo: Distance based on all nodes in CFG (Lower is Better)

👍 🔴 **34.5**

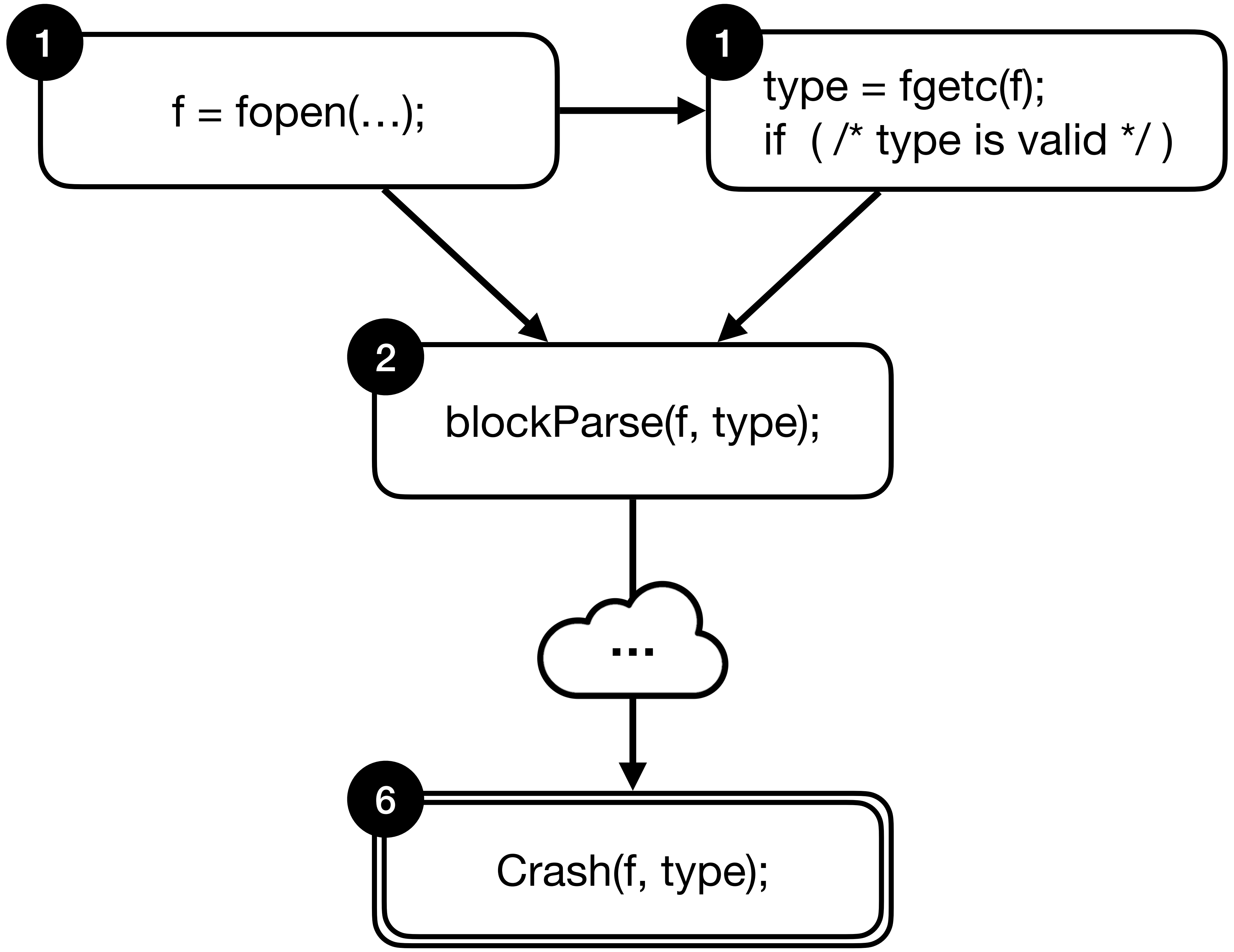
🟢 **37.5**

WindRanger: Distance based on Diverging nodes in CFG (Lower is Better)

👍 🔴 **34**

🟢 **45**

DAFL: Semantic Relevance Score based on DUG (Higher is Better)



*CVE-2017-7578 in swftophp

DAFL's Solution

DUG-based Semantic Relevance Score

AFLGo: Distance based on all nodes in CFG (Lower is Better)

👍 🔴 **34.5**

🟢 **37.5**

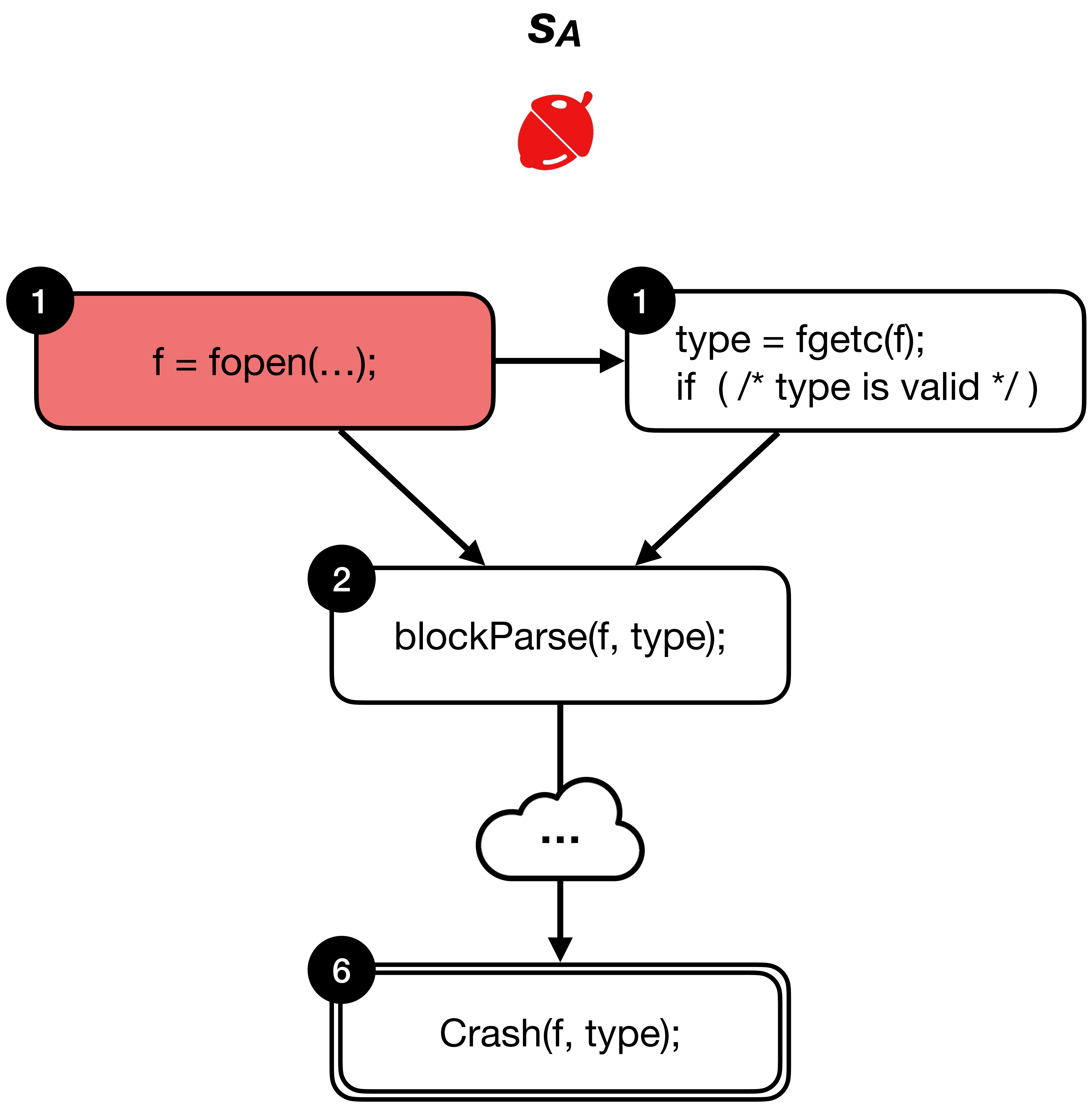
WindRanger: Distance based on Diverging nodes in CFG (Lower is Better)

👍 🔴 **34**

🟢 **45**

DAFL: Semantic Relevance Score based on DUG (Higher is Better)

🔴 **1** Sum(1)



s_A

1 f = fopen(…);

1 type = fgetc(f);
if (/* type is valid */)

2 blockParse(f, type);

…

6 Crash(f, type);

*CVE-2017-7578 in swftophp

DAFL's Solution

DUG-based Semantic Relevance Score

AFLGo: Distance based on all nodes in CFG (Lower is Better)

👍 🟥 **34.5**

🟩 **37.5**

WindRanger: Distance based on Diverging nodes in CFG (Lower is Better)

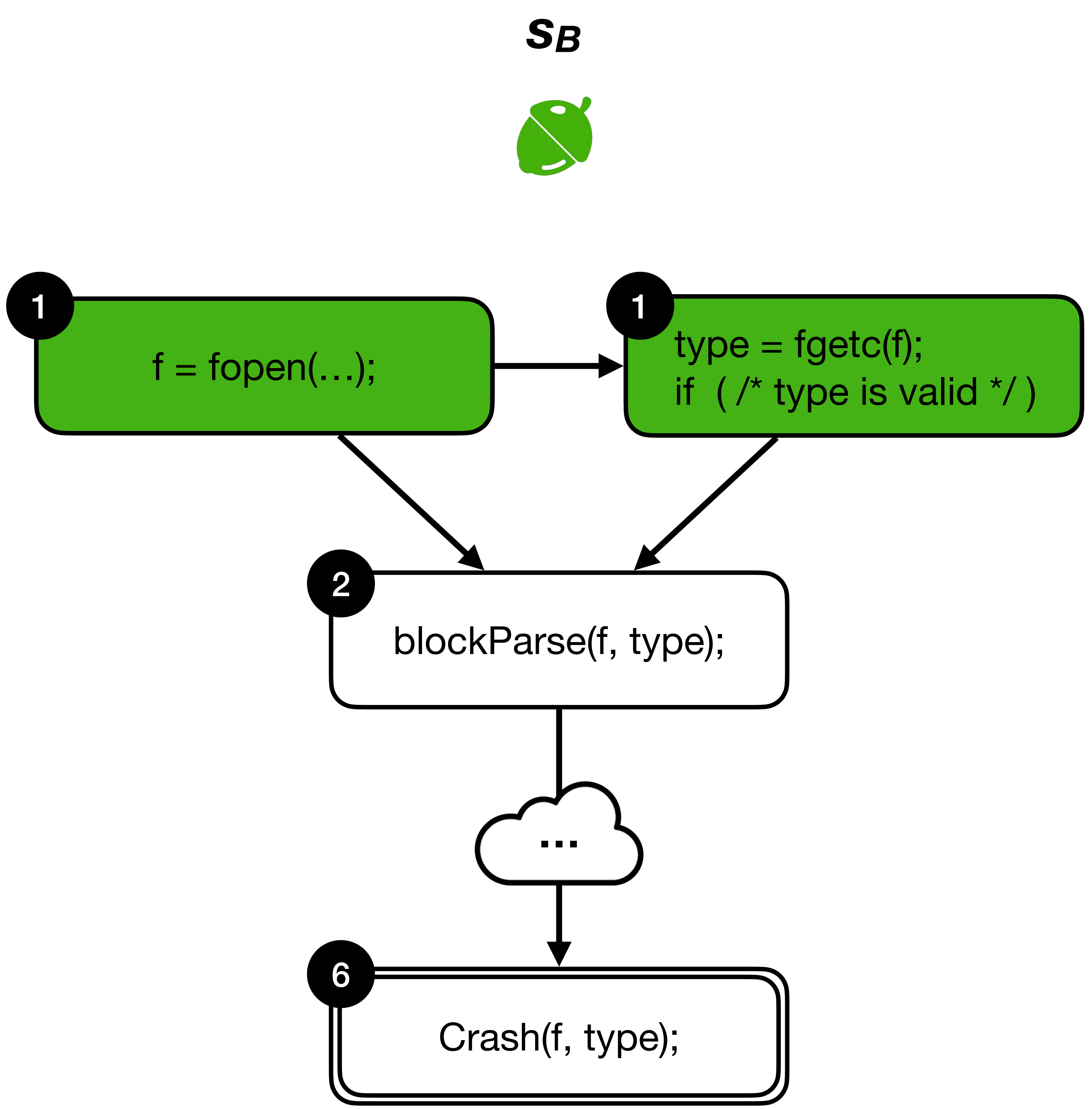
👍 🟥 **34**

🟩 **45**

DAFL: Semantic Relevance Score based on DUG (Higher is Better)

🟥 **1** Sum(1)

👍 🟩 **2** Sum(1, 1)



*CVE-2017-7578 in swftophp

Limitations of DGF

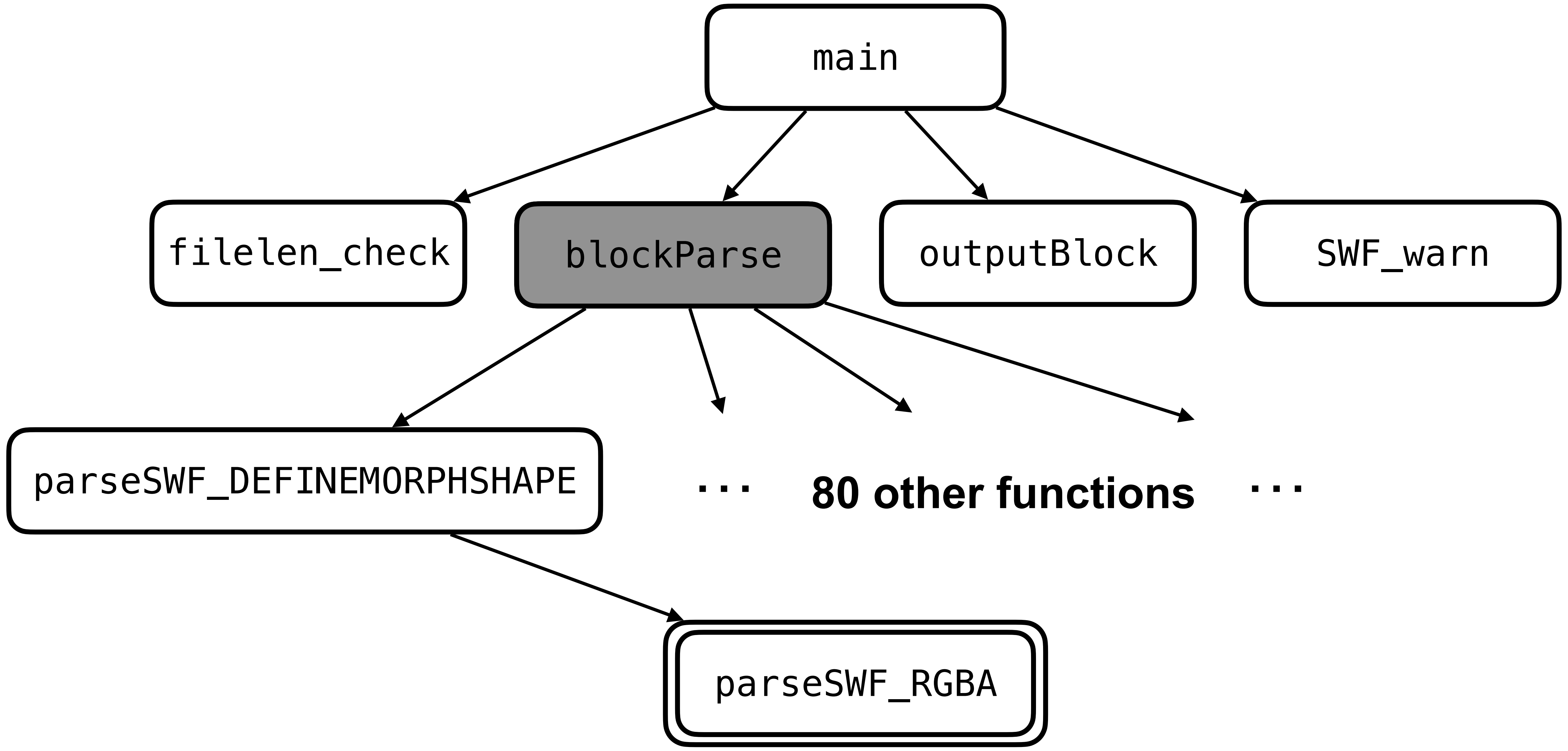
1. **Noisy** seed distance based on Control Flow Graph (CFG)
   - Complex control structures introduce noise in the seed distance

2. **Negative** Coverage Feedback
   - Generate seeds that cover irrelevant program locations

Limitations of DGF

Negative coverage feedback

- Case: CVE-2017-7578 in swftophp

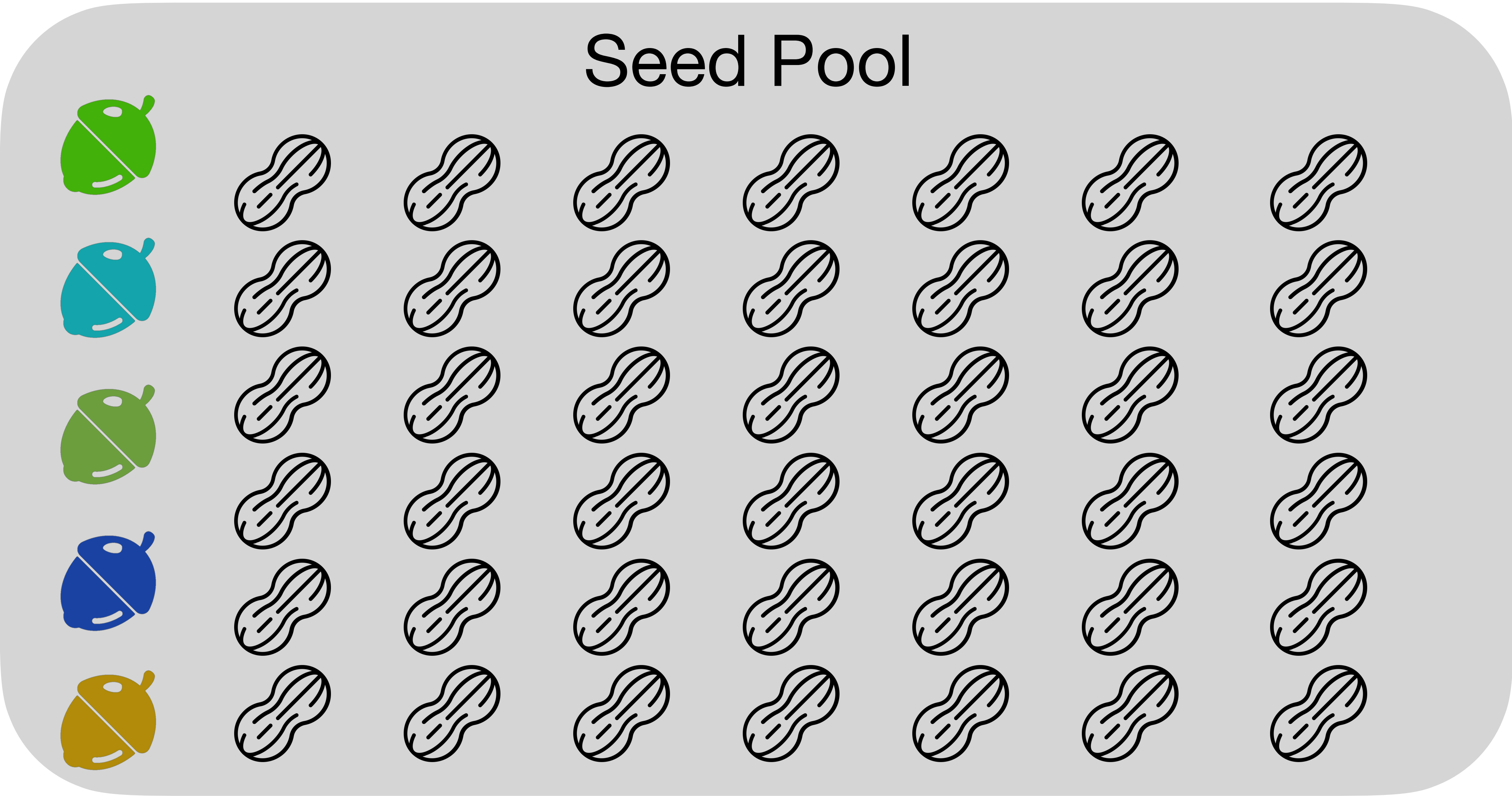


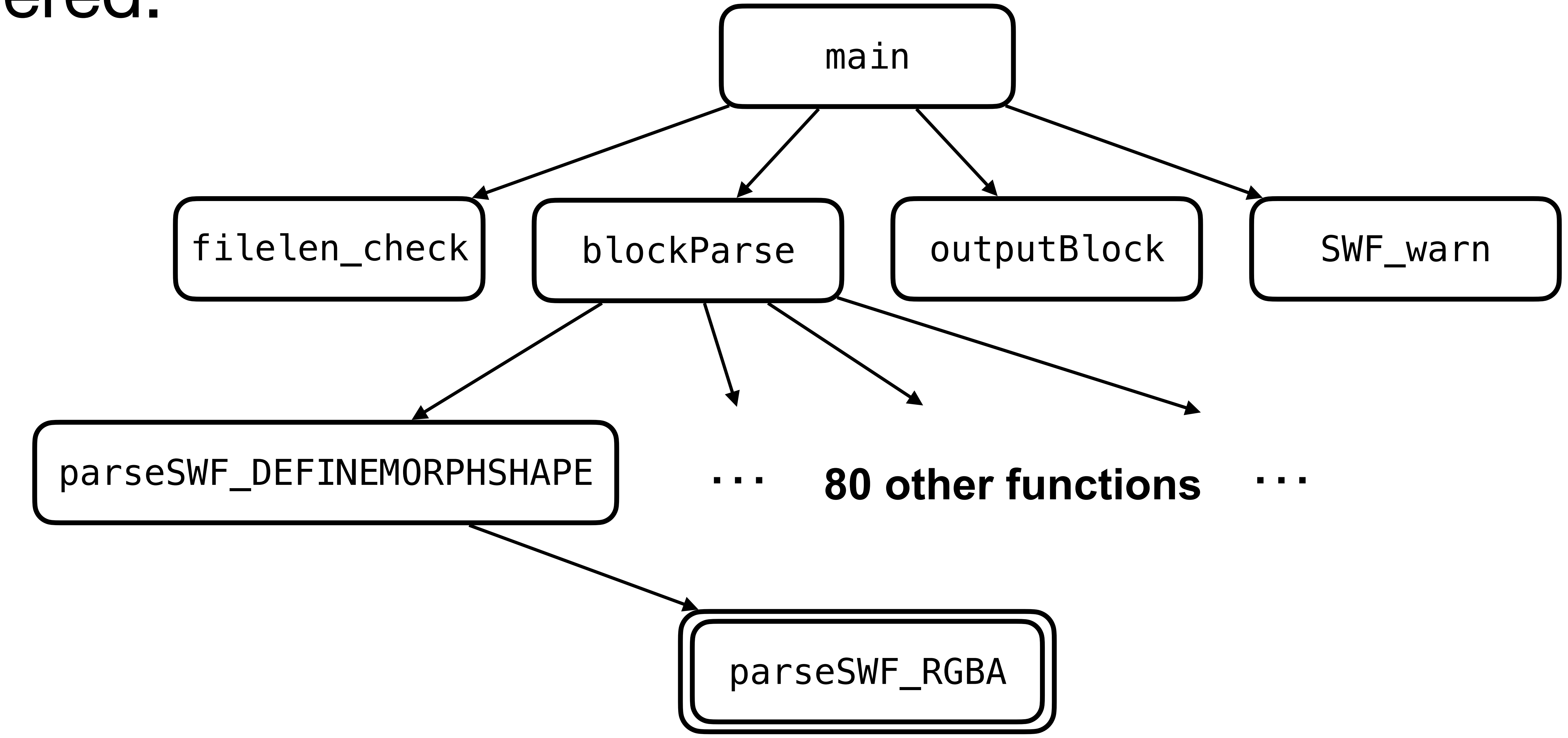
*CVE-2017-7578 in swftophp

Limitations of DGF

Negative coverage feedback

- Case: CVE-2017-7578 in swftophp
- The promising seed is easily outnumbered.





*CVE-2017-7578 in swftophp

DAFL’s Solution

Selective Coverage Instrumentation

- Case: CVE-2017-7578 in swftophp
- The promising seed is easily outnumbered.

Seed Pool

DAFL selectively receives coverage feedback by

<u>Selective Coverage Instrumentation</u>

main
filelen_check
blockParse
outputBlock
SWF_warn
parseSWF_DEFINEMORPHSHAPE
···
80 other functions
···
parseSWF_RGBA

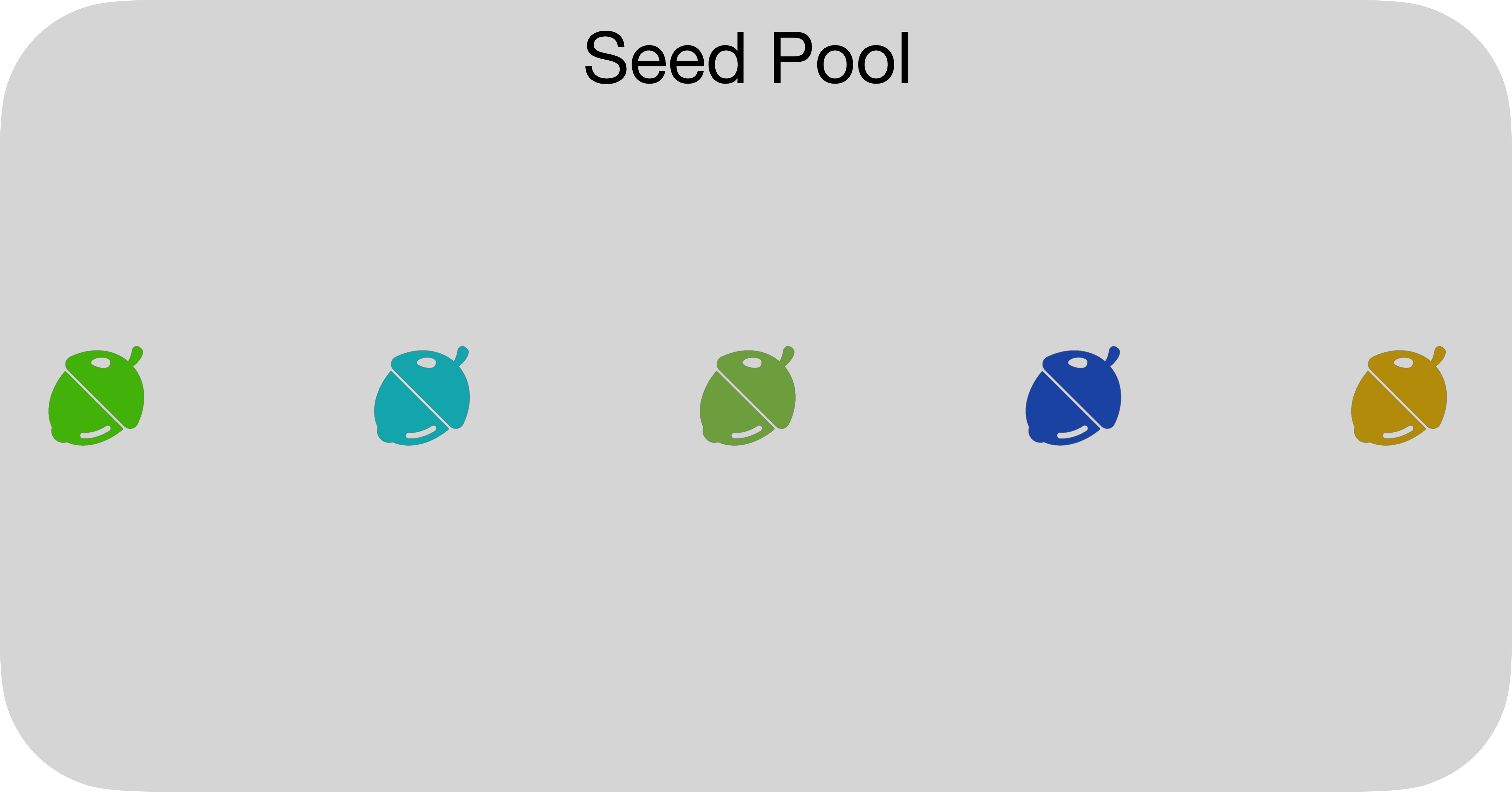
쪽수를 가운데로, 주석을 현재 쪽수 위치로

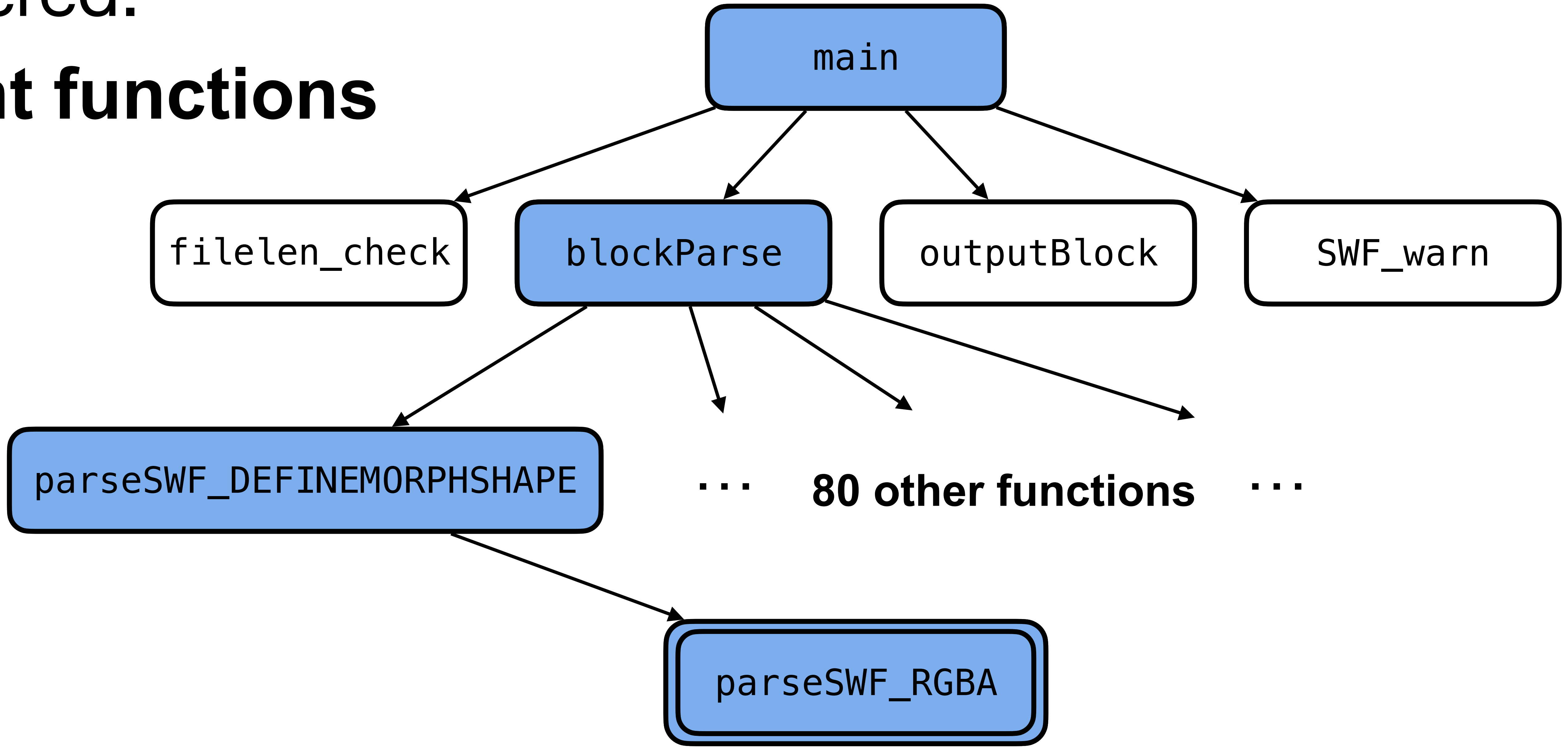
DAFL's Solution

Selective Coverage Instrumentation

- Case: CVE-2017-7578 in swftophp
- ~~The promising seed is easily outnumbered.~~

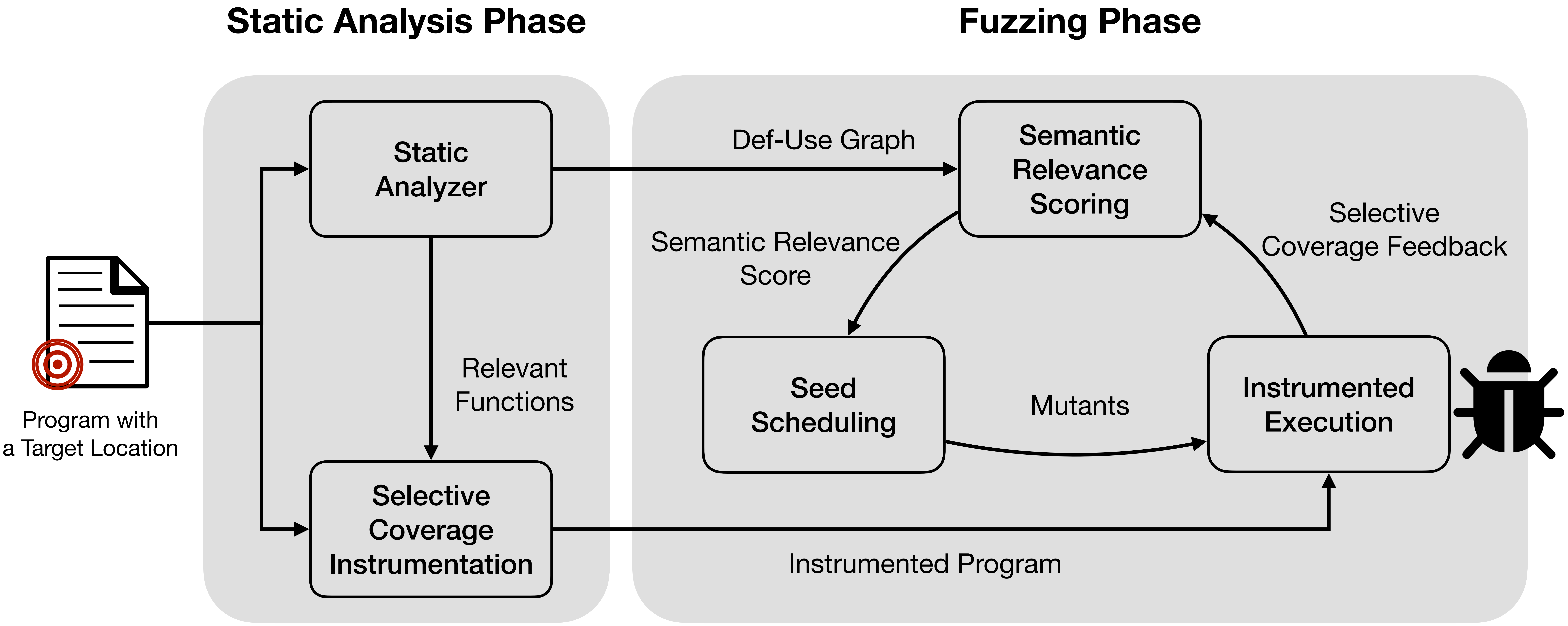
No seeds are generated from irrelevant functions



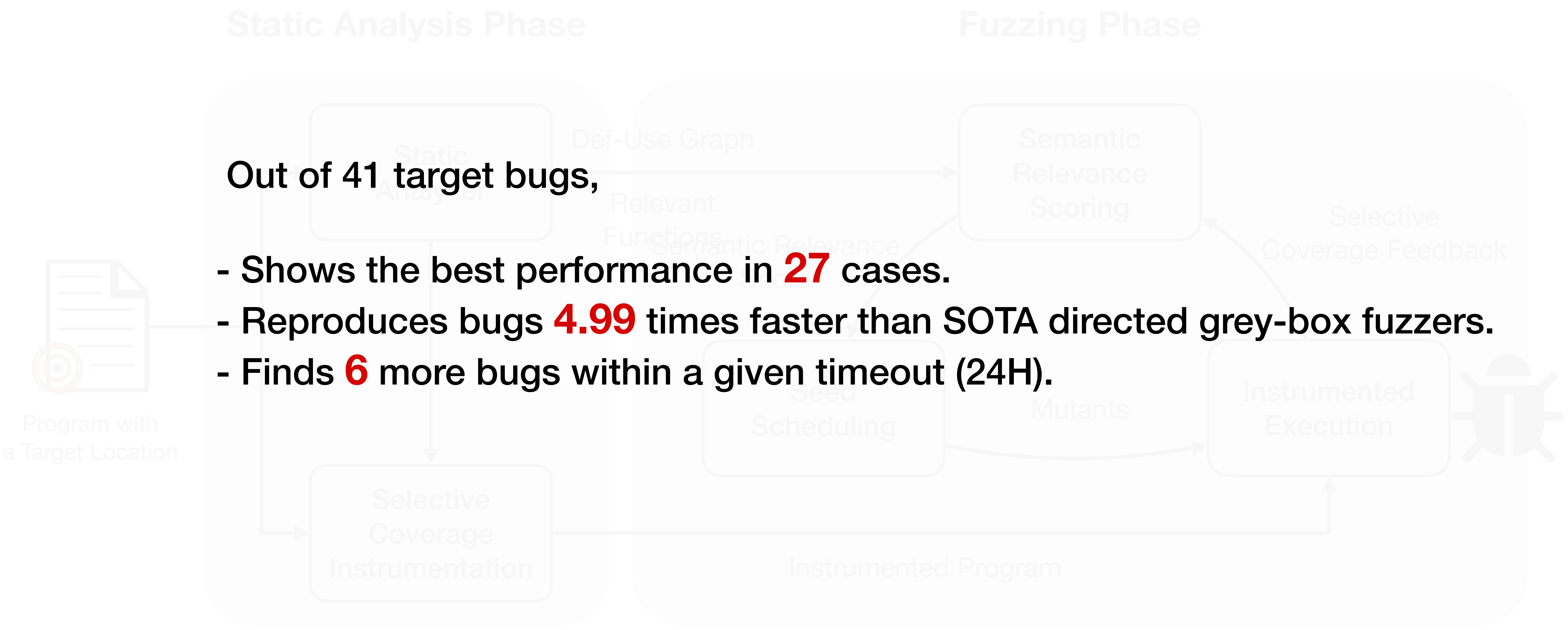


*CVE-2017-7578 in swftophp

DAFL Overview



DAFL Overview



Out of 41 target bugs,

- Shows the best performance in **27** cases.
- Reproduces bugs **4.99** times faster than SOTA directed grey-box fuzzers.
- Finds **6** more bugs within a given timeout (24H).

Evaluation

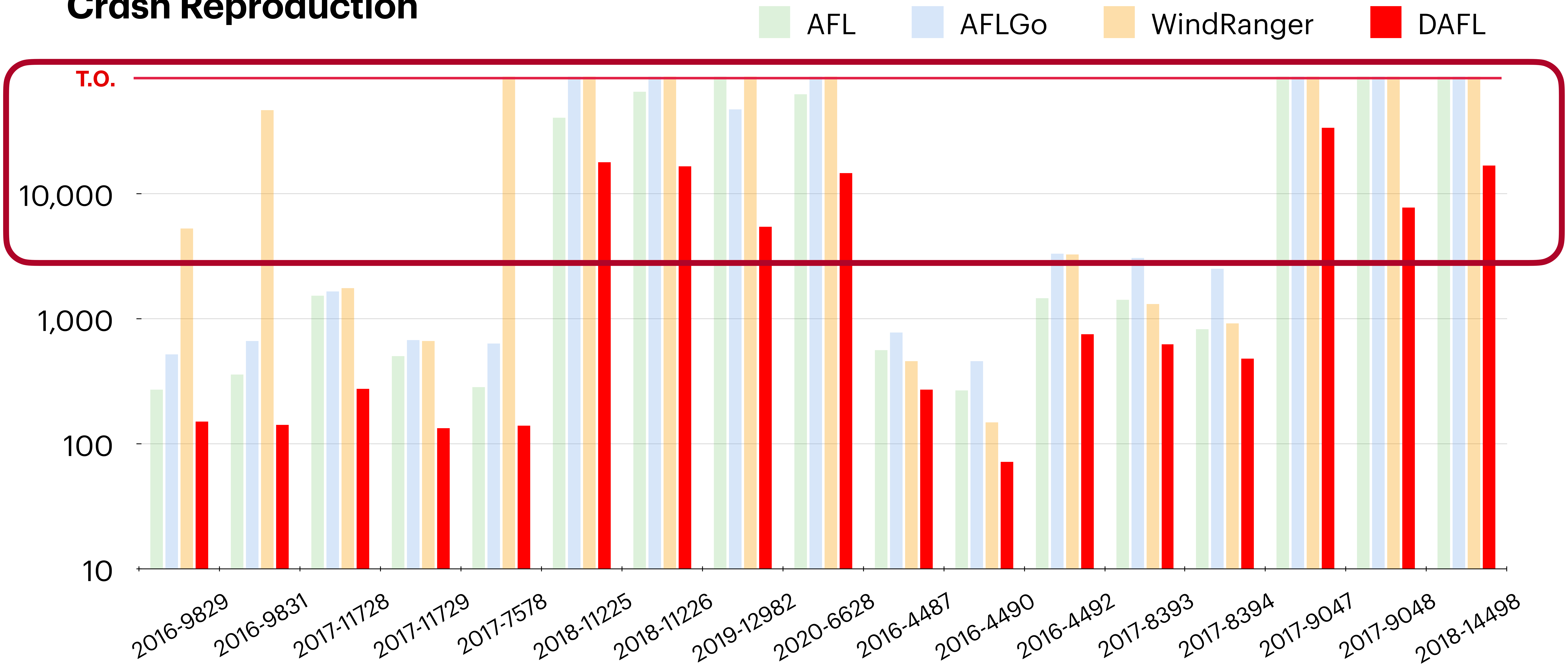
Crash Reproduction

- Benchmark
  - 41 CVEs from 10 programs
- Baselines
  - 1 Undirected Fuzzer
    - AFL
  - 3 Directed Fuzzers
    - AFLGo
    - WindRanger
    - Beacon
- Criteria
  - Median time of 40 iterations to reproduce the target bug

Evaluation

Best performance in 27 cases.
4.99 times faster than the baseline DGF
Finds 6 more bugs within a given timeout (24H).

Crash Reproduction



Summary

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED

Link to our artifact!!

- **Directed Grey-box Fuzzing**
  - Limitations
    - Noisy Seed Distance
    - Negative Coverage Feedback

- **Solution: DAFL**
  - Directed Grey-box Fuzzing Guided by Data Dependency

- **Key Concepts of DAFL**
  - Semantic Relevance Scoring
  - Selective Coverage Instrumentation

→ Achieves 4.99 times performance boost against the SOTA Directed Grey-box Fuzzers