GeneVis:

A Genealogical Visualization Tool for Directed Grey-box Fuzzing

Tae Eun Kim

KAIST

Background

Background

Fuzzing

- Testing a program with randomly generated inputs

Background

Fuzzing

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

Background

Fuzzing

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

Directed Grey-box Fuzzing

Background

Fuzzing

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

Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)

Background

Fuzzing

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

Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program

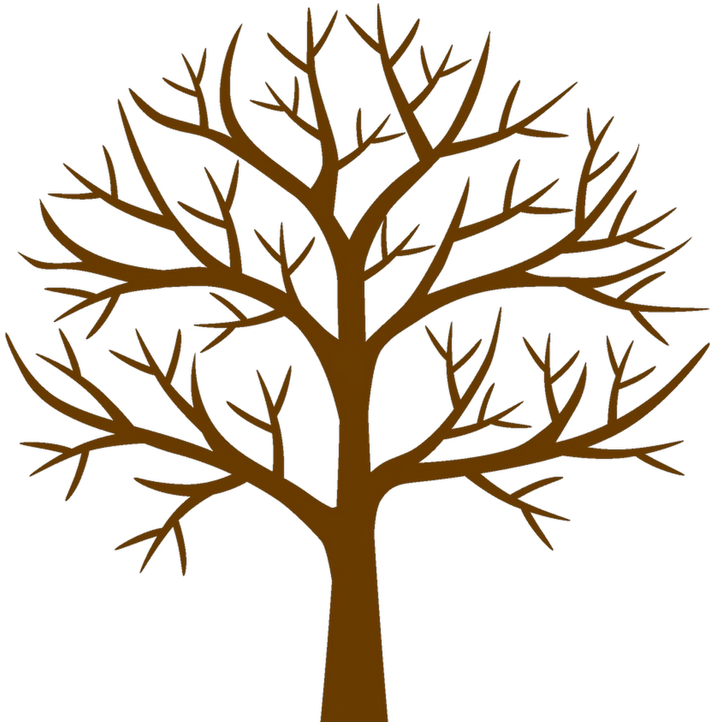
Background

Fuzzing

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

Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program



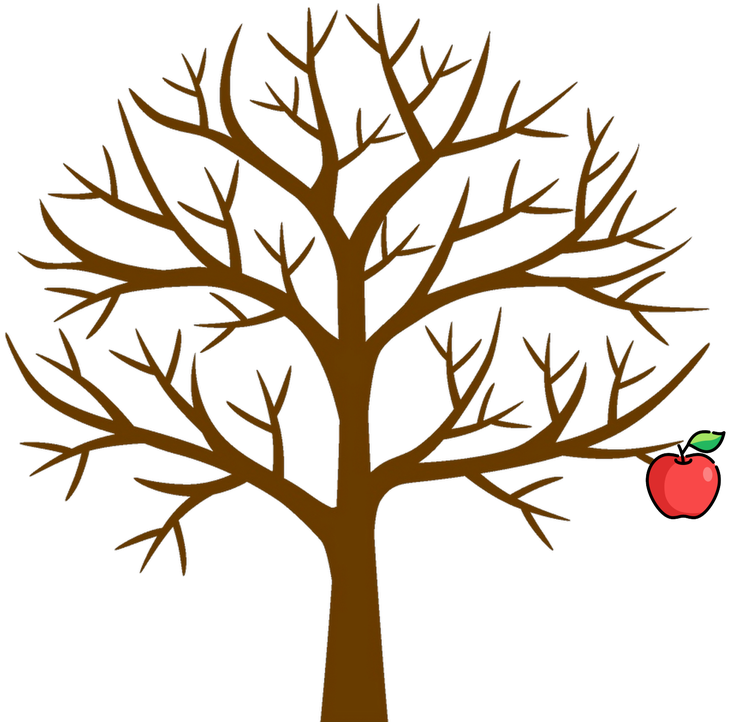
Background

Fuzzing

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

Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program



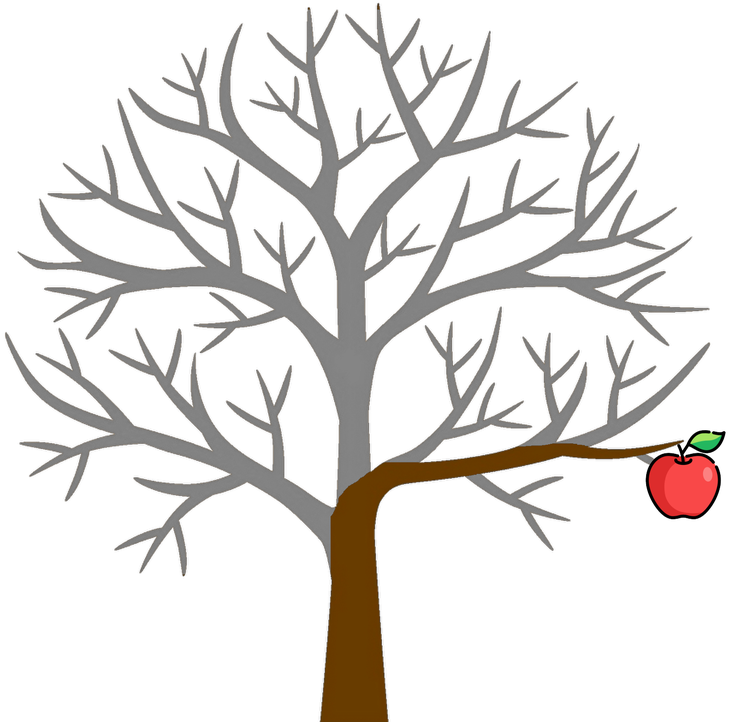
Background

Fuzzing

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

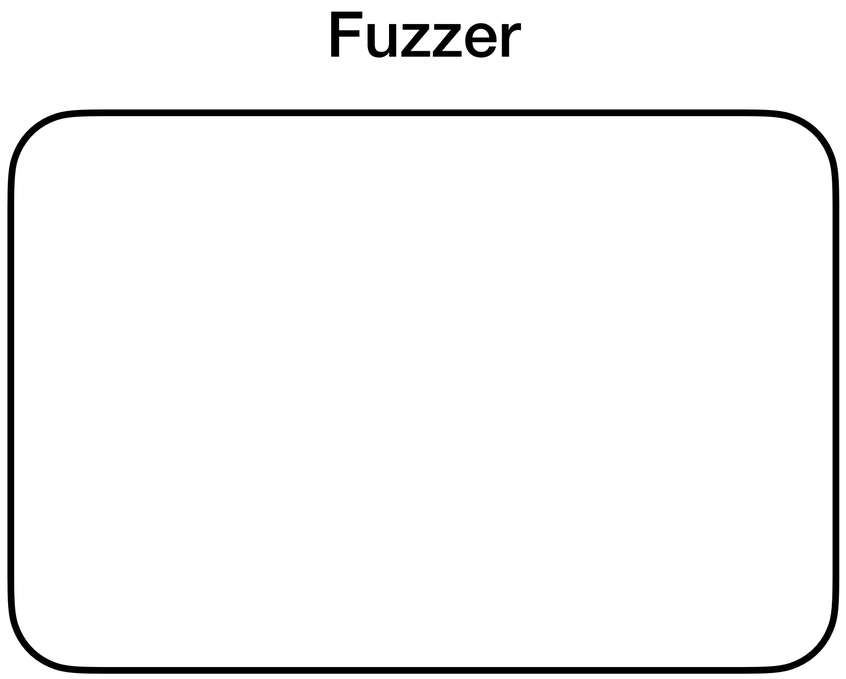
Directed Grey-box Fuzzing

- Directed: Aims to reach the given target location(s)
- Grey-box: Utilize coverage to explore the program

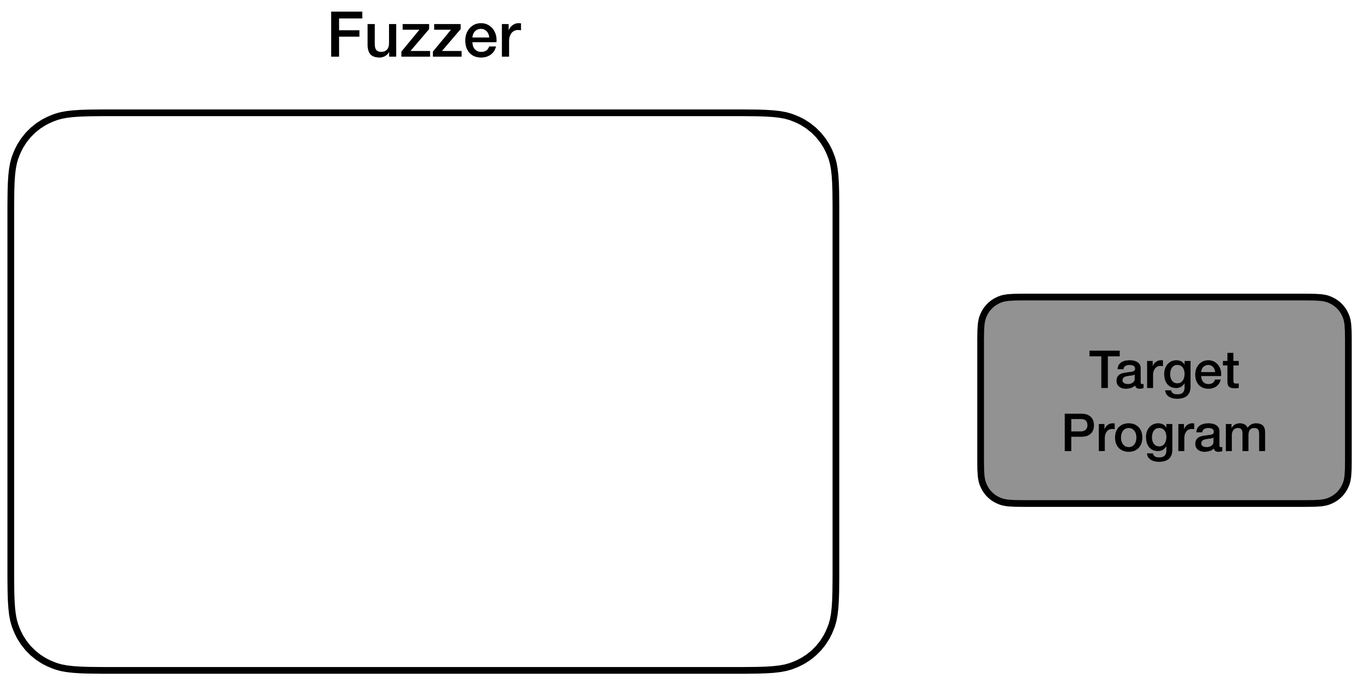


Grey-box Fuzzing

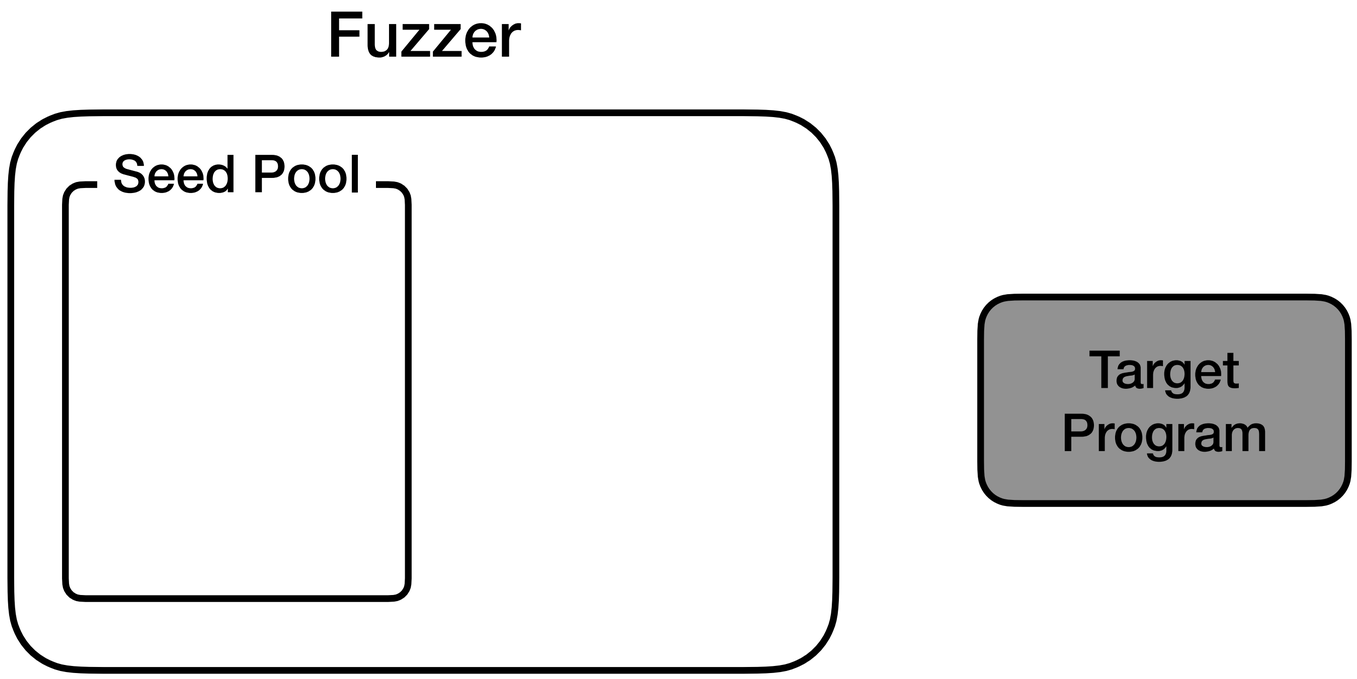
Grey-box Fuzzing



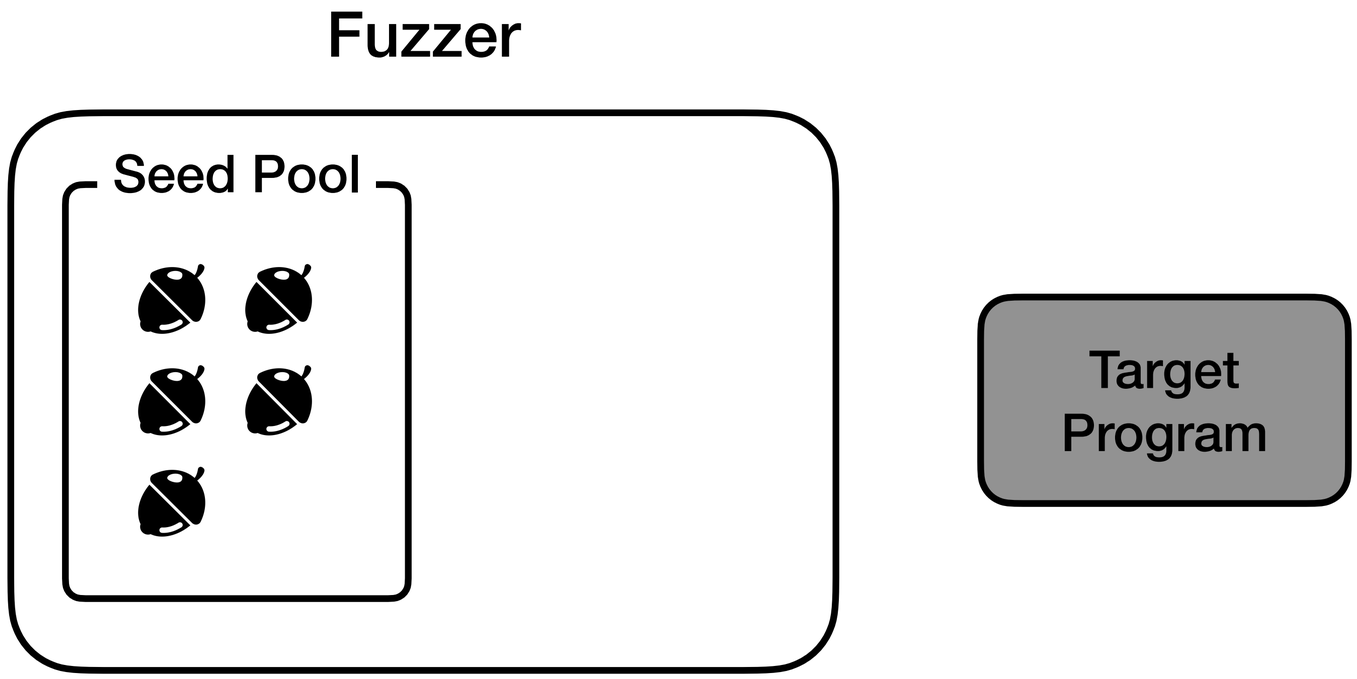
Grey-box Fuzzing



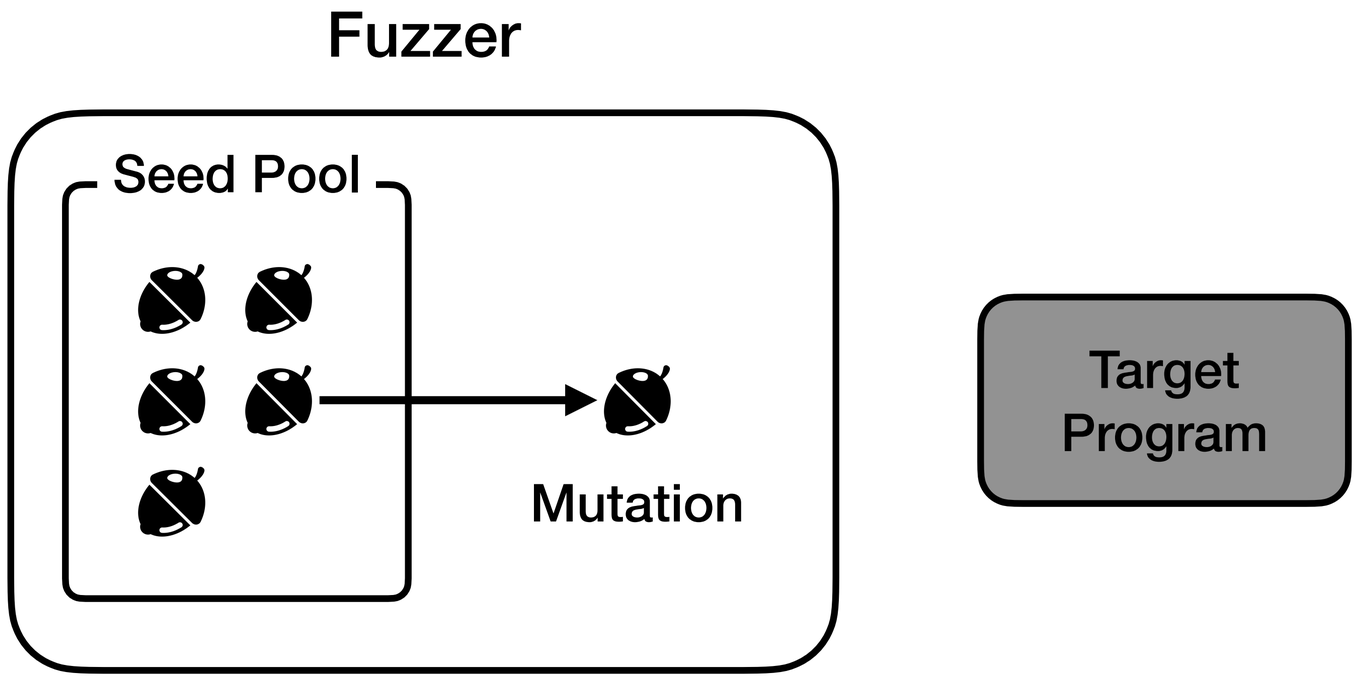
Grey-box Fuzzing



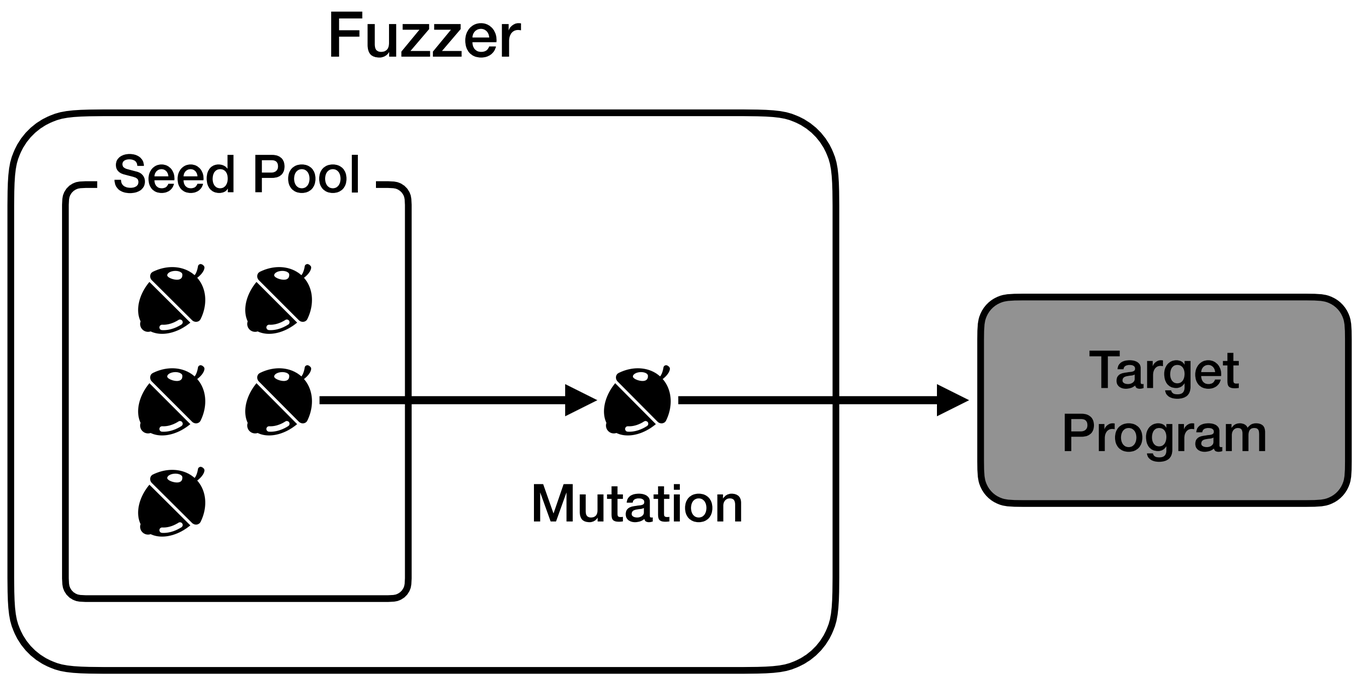
Grey-box Fuzzing



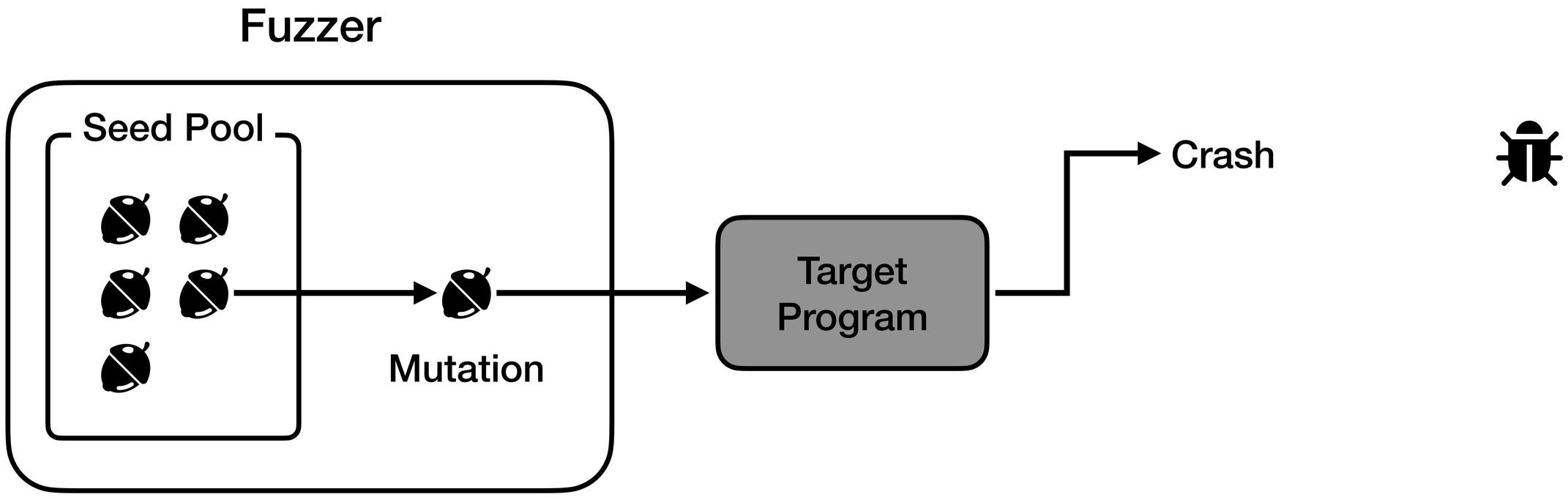
Grey-box Fuzzing



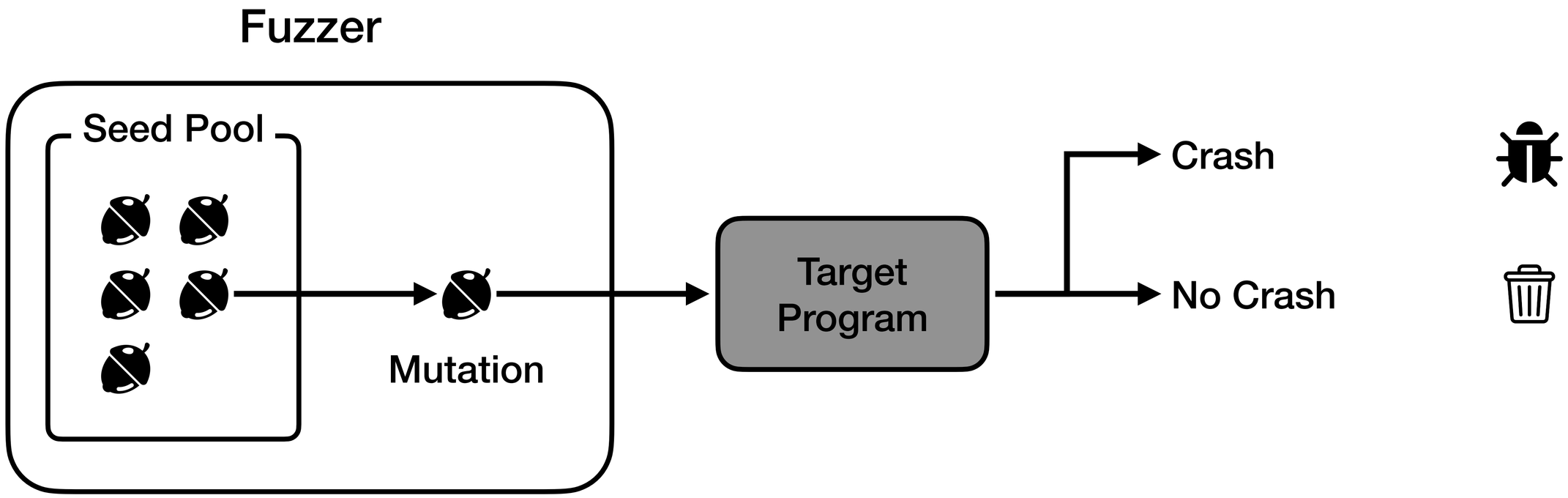
Grey-box Fuzzing



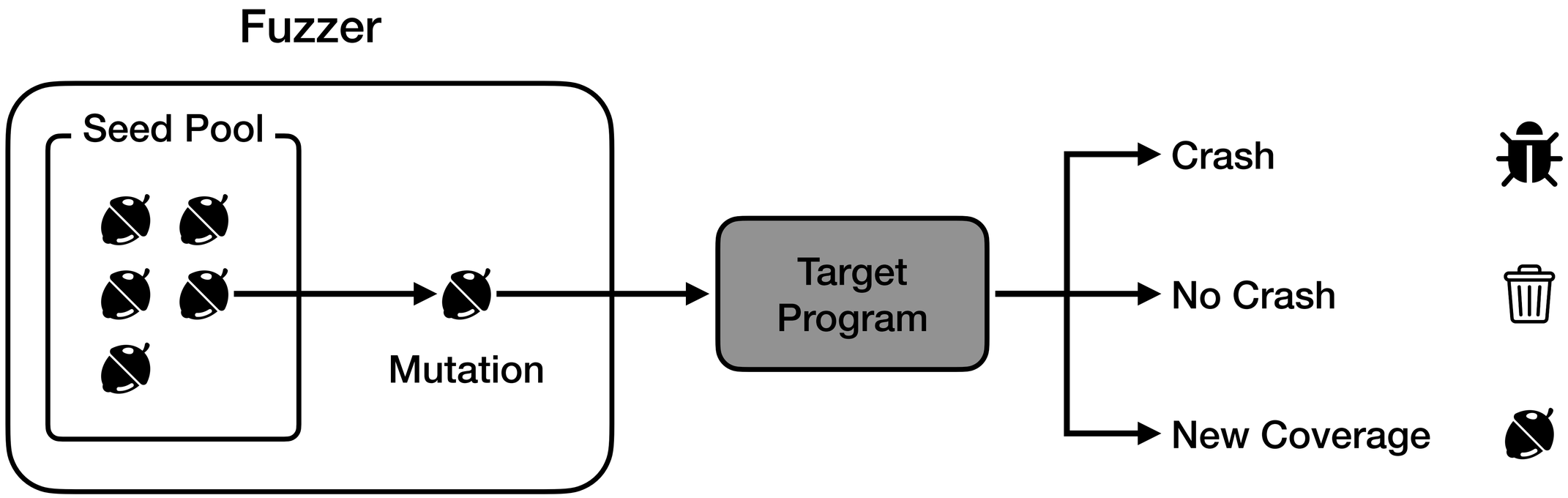
Grey-box Fuzzing



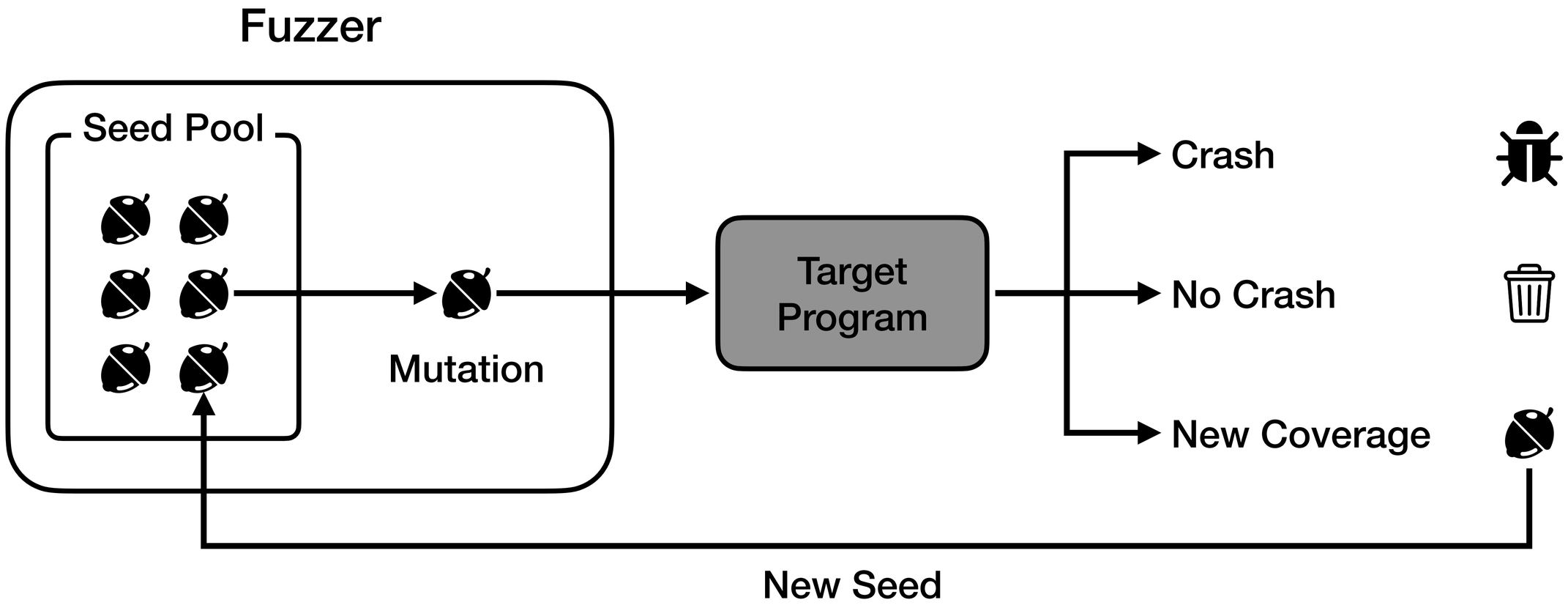
Grey-box Fuzzing



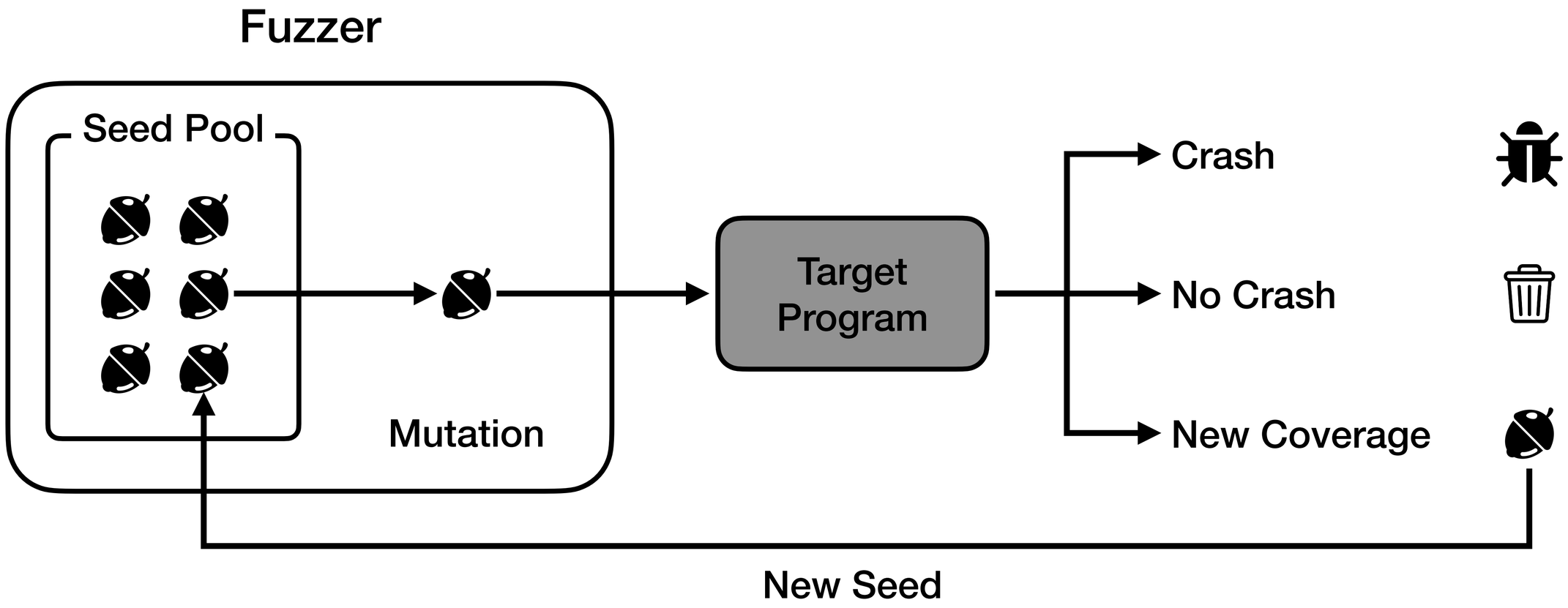
Grey-box Fuzzing



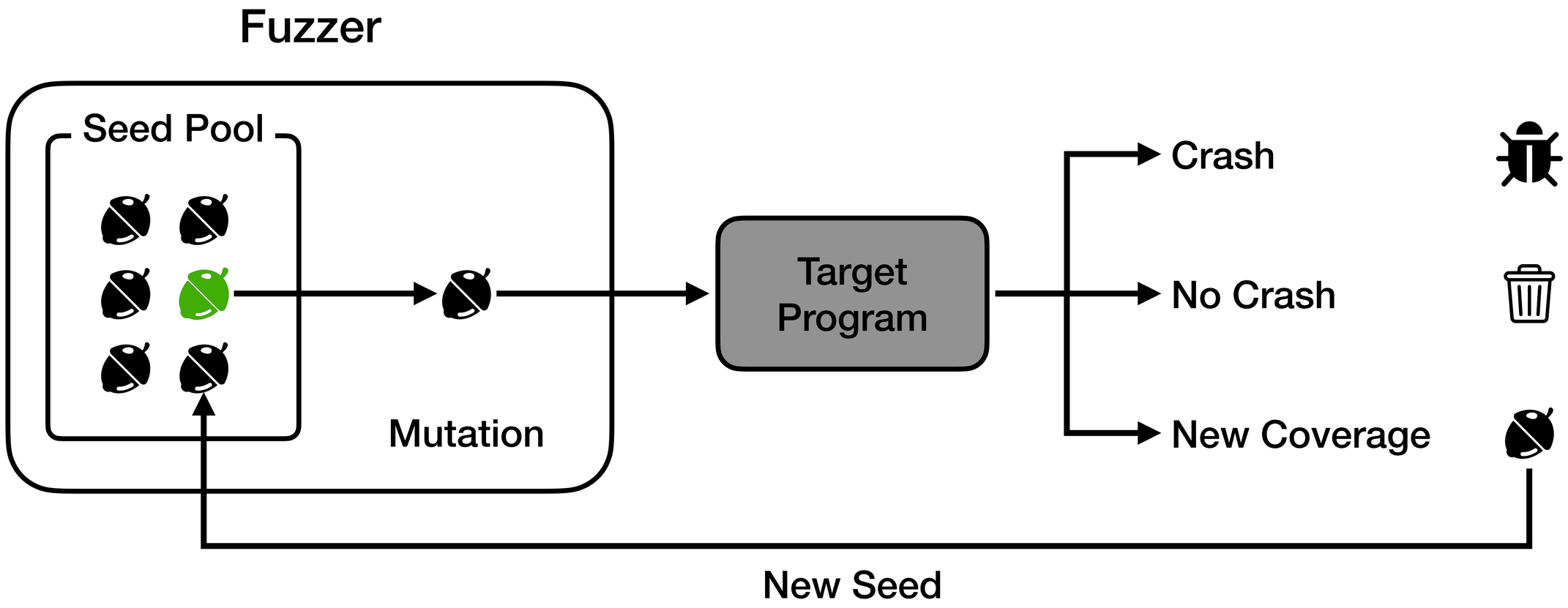
Grey-box Fuzzing



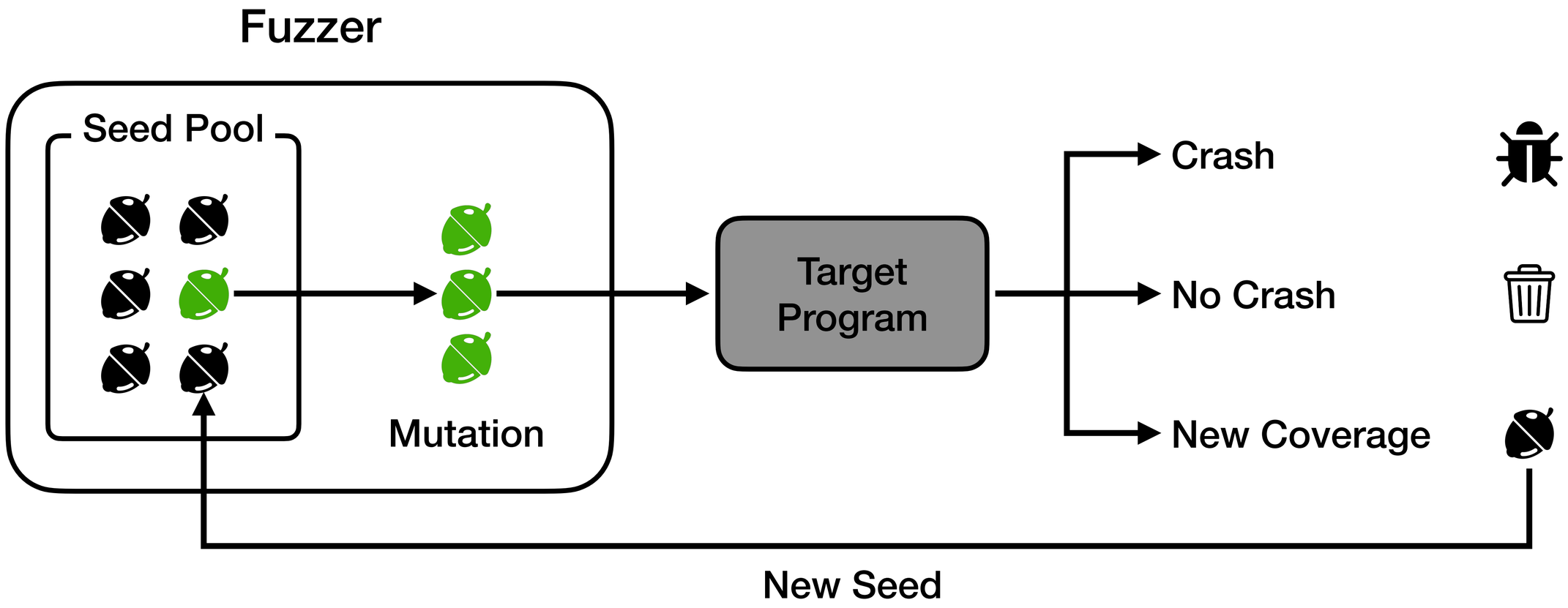
Directed Grey-box Fuzzing



Directed Grey-box Fuzzing



Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

Analysis of Directed Grey-box Fuzzing

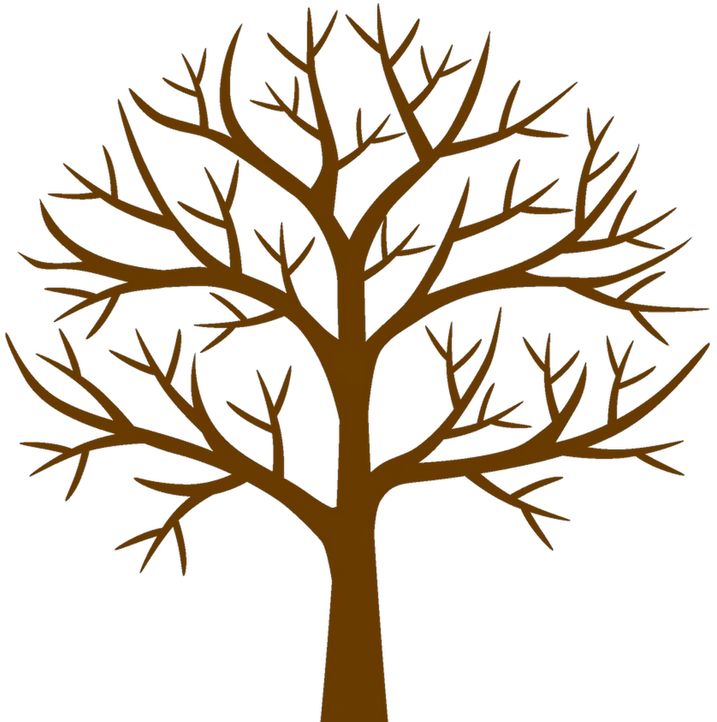
Progress of Fuzzing

- Each seed represents each step into the program

Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

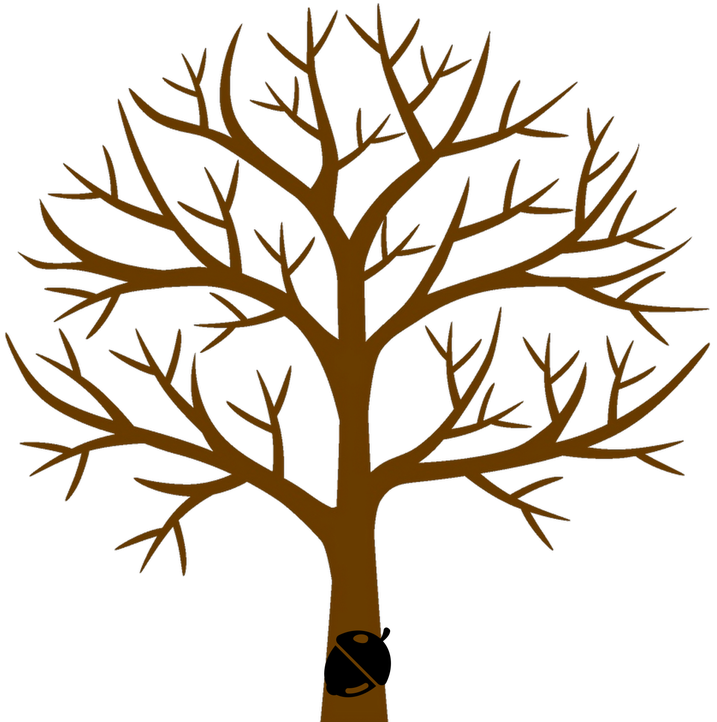
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

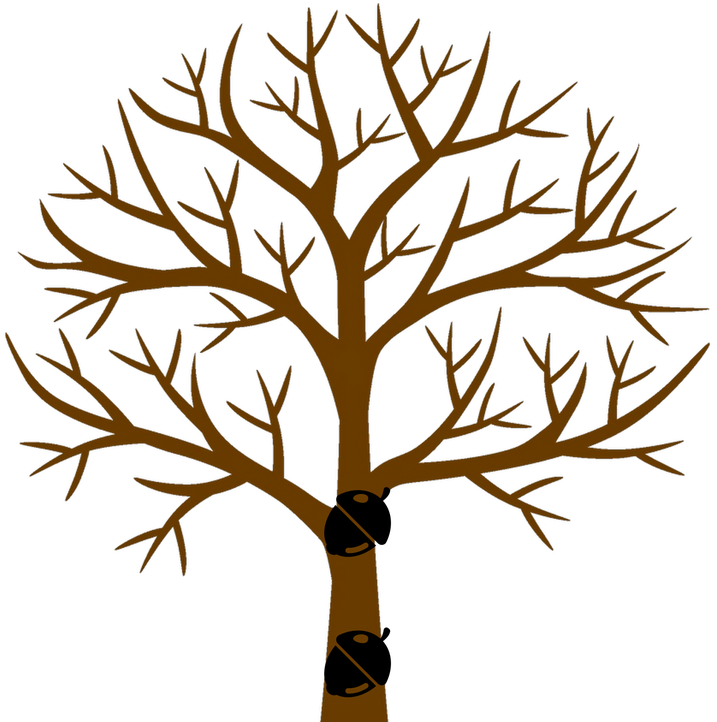
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

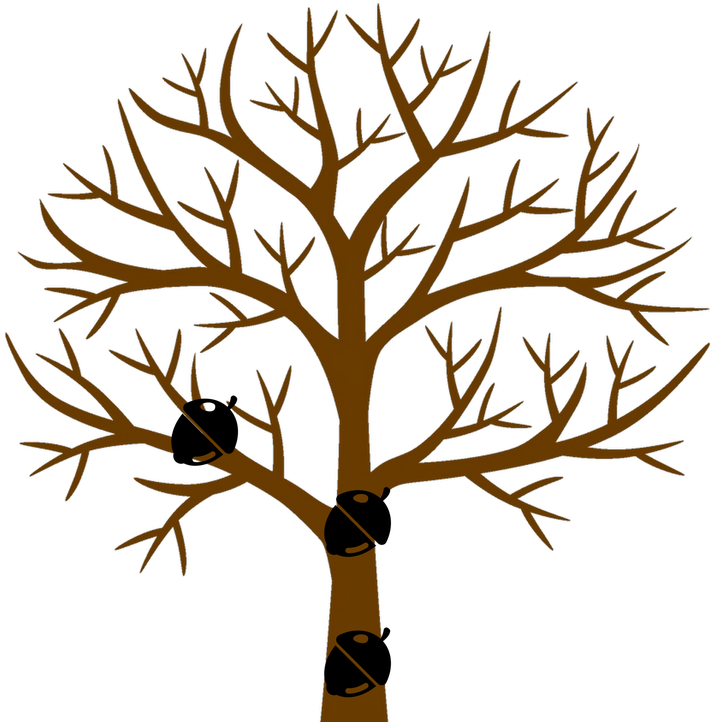
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

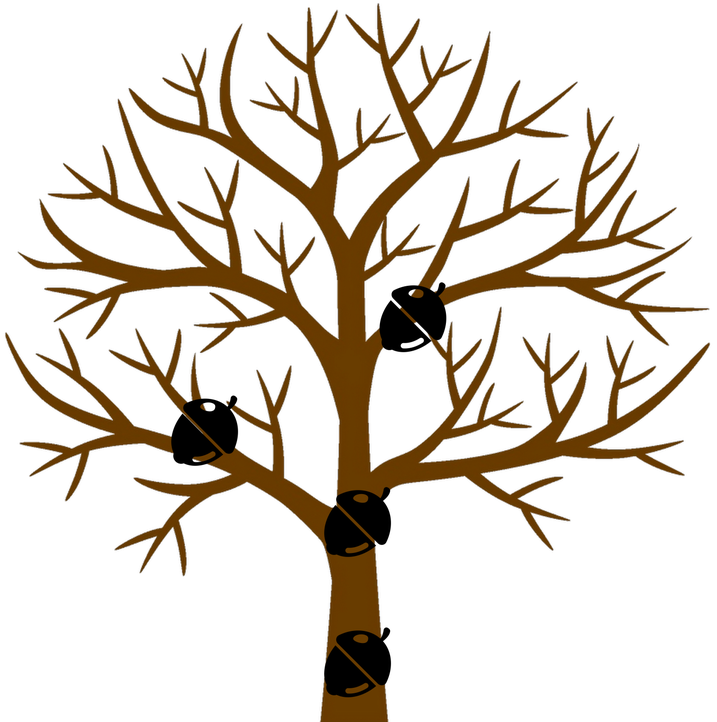
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

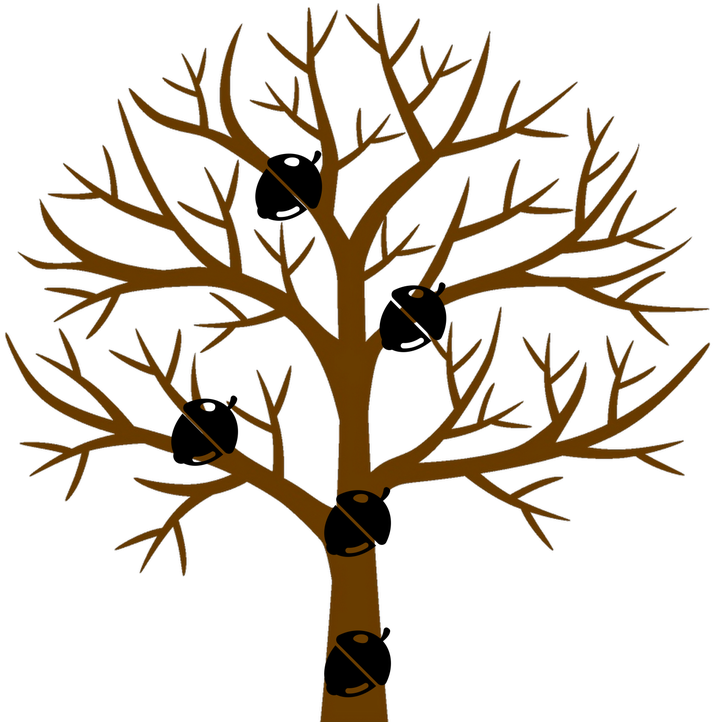
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

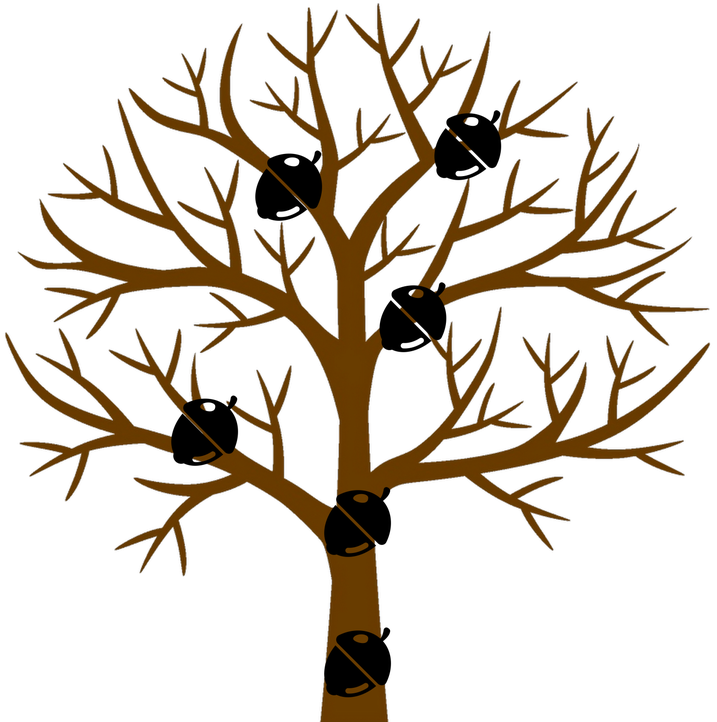
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

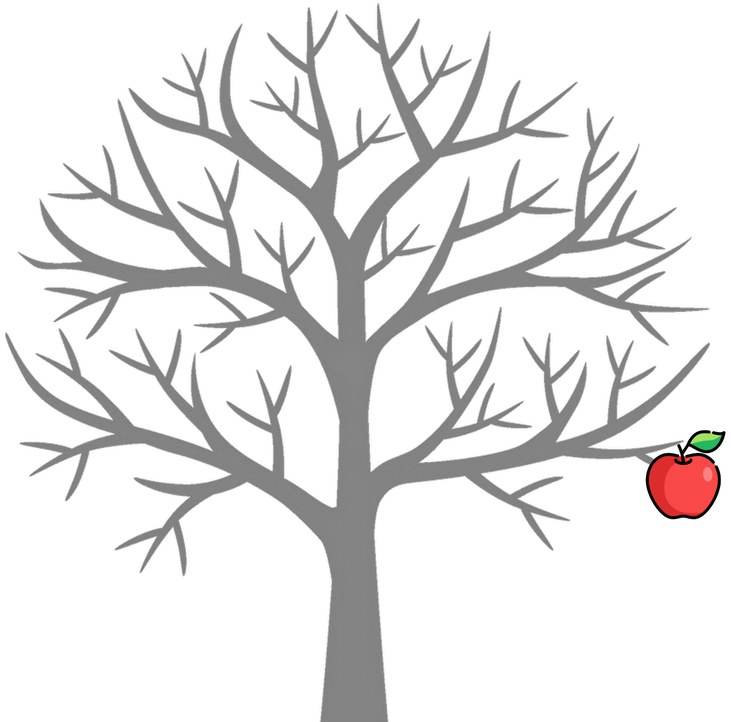
- Each seed represents each step into the program



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

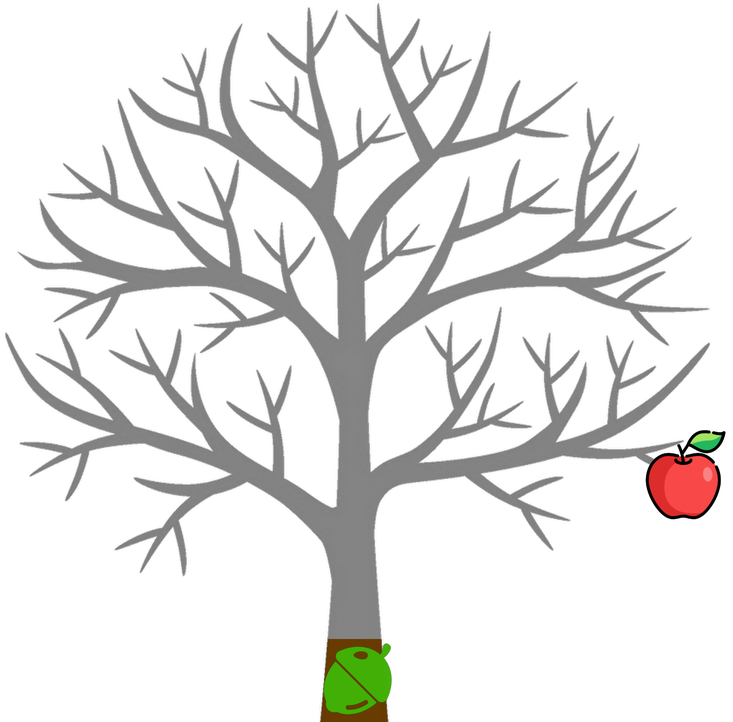
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

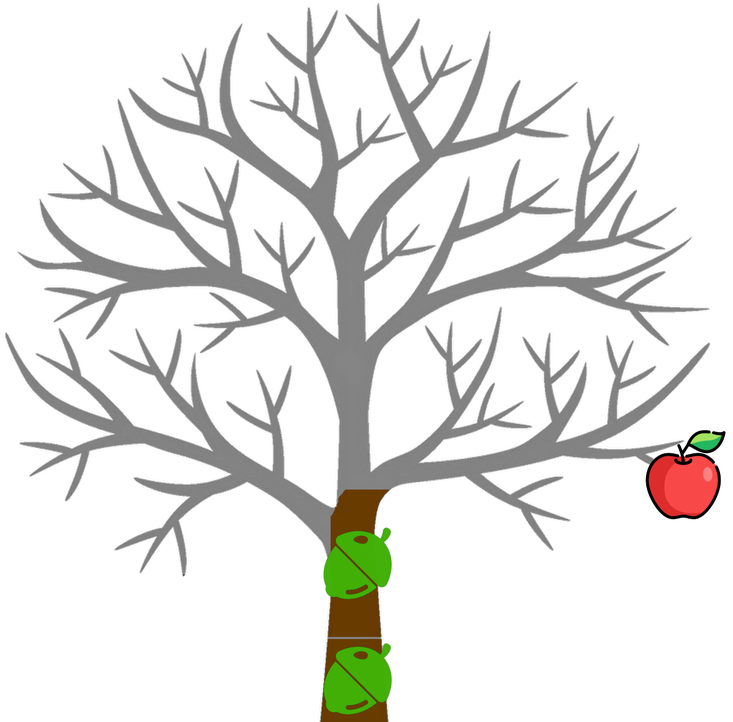
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

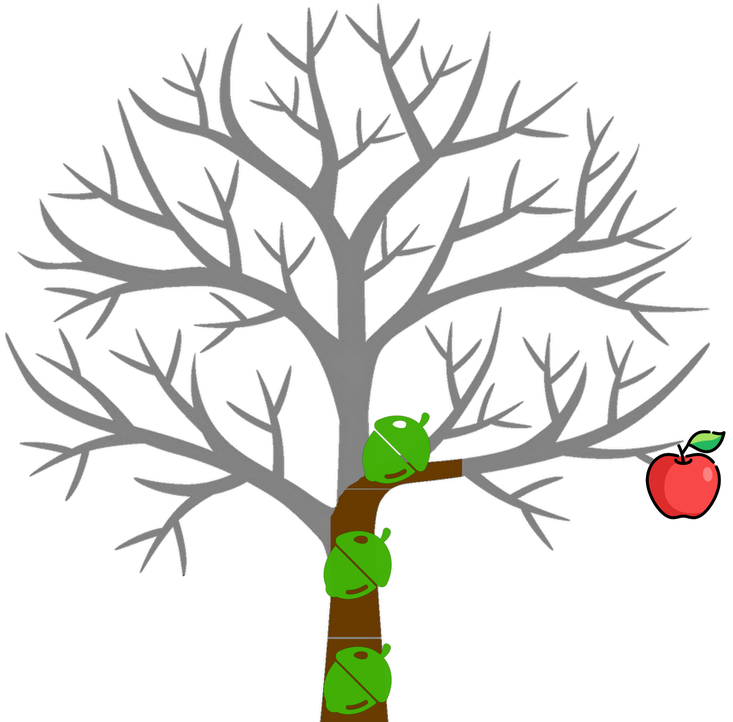
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

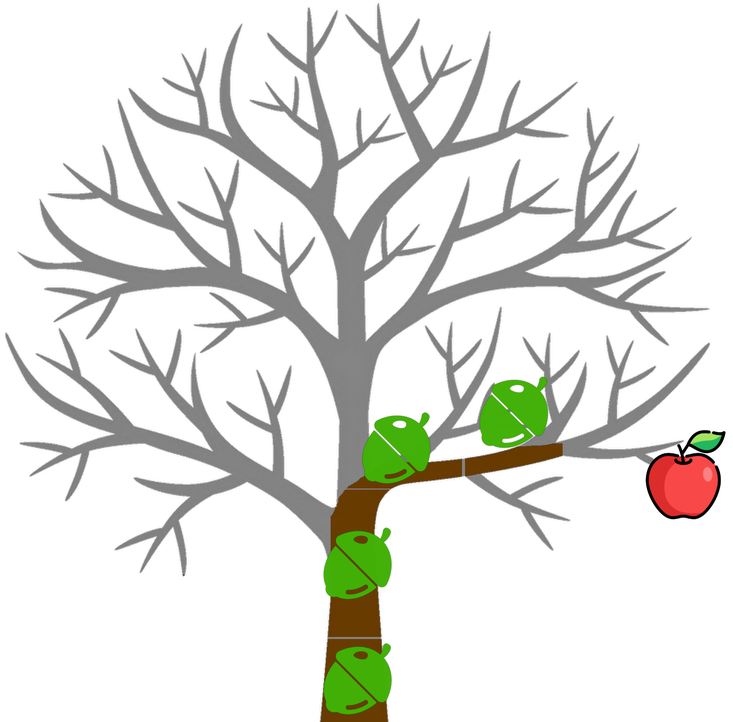
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

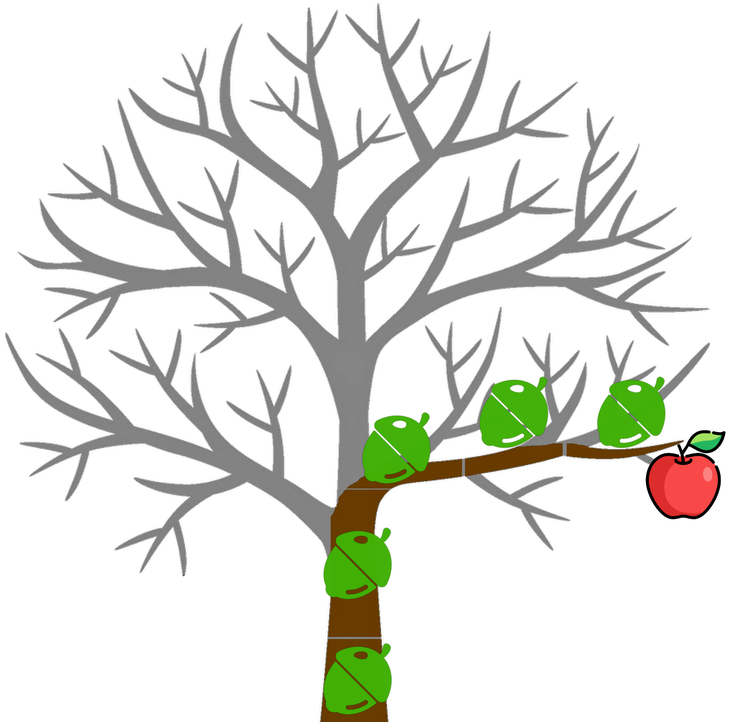
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

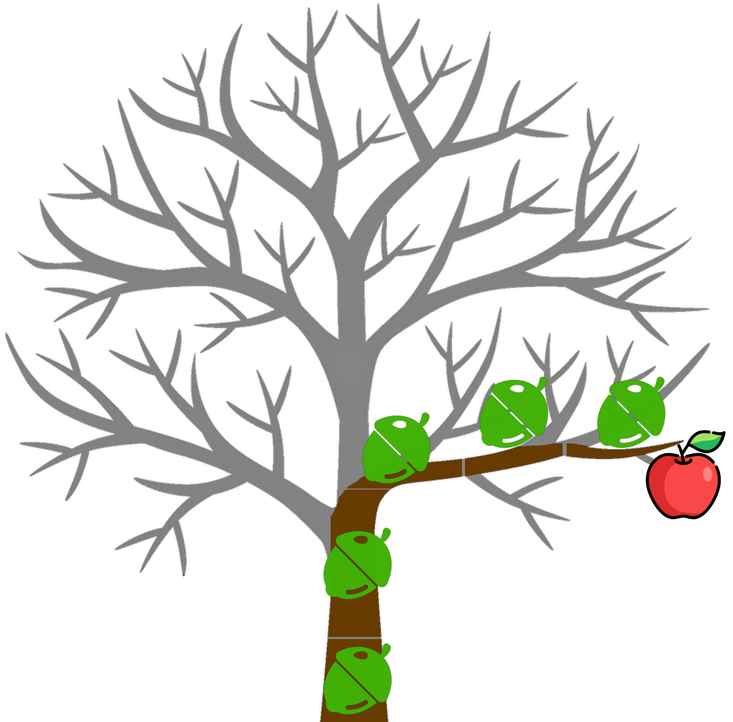
- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing



Analysis of Directed Grey-box Fuzzing

Progress of Fuzzing

- Each seed represents each step into the program
- Each step is especially important in Directed Grey-box Fuzzing
- Understanding the steps of progress is crucial



Challenge

Challenge

Grey-box fuzzer is a black box

Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of

Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of

Number of inputs generated in 24 hours by DAFL[1]

Program	All Inputs	Seed Inputs	Crashing Inputs
swftophp	24,727,449	3,839	421
lrzip	4,610,069	676	44
cxxfilt	14,784,726	4,657	346
objcopy	23,562,580	5,207	177
objdump	21,022,357	5,863	175
strip	131,633	1,018	6
nm	5,976,949	2,345	69
readelf	89,493	774	1
xmllint	63,012,643	1,283	2
cjpeg	18,245,672	4,650	20
Average	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection

Number of inputs generated in 24 hours by DAFL[1]

Program	All Inputs	Seed Inputs	Crashing Inputs
swftophp	24,727,449	3,839	421
lrzip	4,610,069	676	44
cxxfilt	14,784,726	4,657	346
objcopy	23,562,580	5,207	177
objdump	21,022,357	5,863	175
strip	131,633	1,018	6
nm	5,976,949	2,345	69
readelf	89,493	774	1
xmllint	63,012,643	1,283	2
cjpeg	18,245,672	4,650	20
Average	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Number of inputs generated in 24 hours by DAFL[1]

Program	All Inputs	Seed Inputs	Crashing Inputs
swftophp	24,727,449	3,839	421
lrzip	4,610,069	676	44
cxxfilt	14,784,726	4,657	346
objcopy	23,562,580	5,207	177
objdump	21,022,357	5,863	175
strip	131,633	1,018	6
nm	5,976,949	2,345	69
readelf	89,493	774	1
xmllint	63,012,643	1,283	2
cjpeg	18,245,672	4,650	20
Average	17,616,357	3,031	126

1. “DAFL : Directed Grey-Box Fuzzing Guided by Data Dependency”, Kim et al., USENIX Security 2023

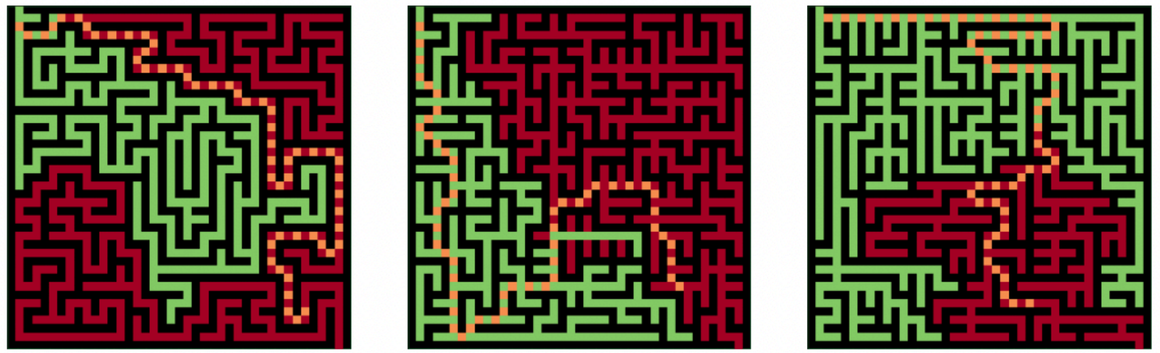
Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Visualization Tools

Challenge



Visualization of Fuzzle[1]

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Visualization Tools

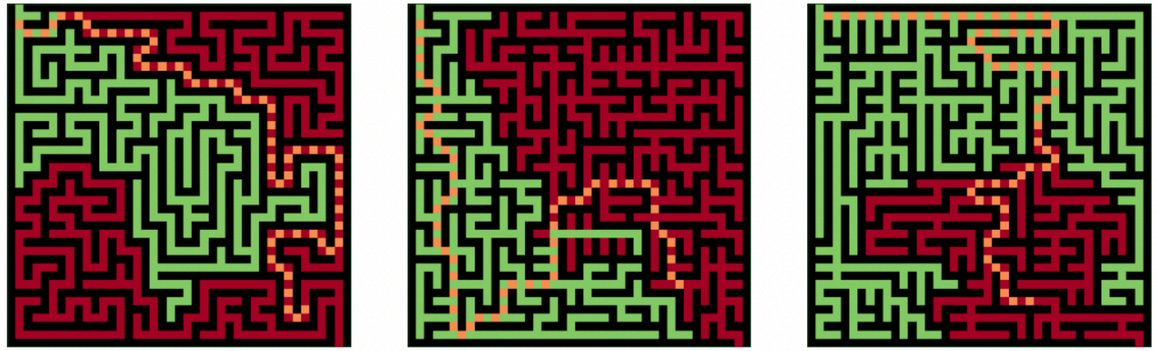
1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022

Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Visualization Tools



Visualization of Fuzzle[1]

LCOV - code coverage report

			Hit	Total	Coverage
Current view:	top level	**Lines:**	3270	7970	41.0 %
Test:	id:002084,src:002034,op:havoc,rep:2.lcov_info_final	**Functions:**	224	390	57.4 %
Date:	2015-05-25	**Branches:**	1778	5269	33.7 %

Directory	Line Coverage		Functions		Branches	
server	28.4 %	876 / 3080	39.5 %	49 / 124	27.0 %	541 / 2007
client	33.8 %	690 / 2039	54.9 %	39 / 71	31.5 %	397 / 1260
lib	59.8 %	1704 / 2851	69.7 %	136 / 195	42.0 %	840 / 2002

Generated by: LCOV version 1.10

Visualization of afl-cov[2]

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. “afl-cov - AFL Fuzzing Code Coverage”, Rash

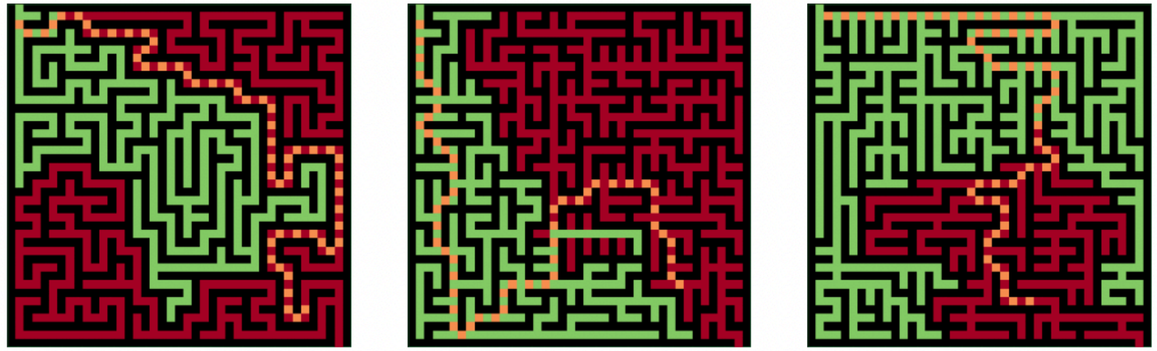
Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Visualization Tools

- Focused on coverage analysis



Visualization of Fuzzle[1]

LCOV - code coverage report

			Hit	Total	Coverage
Current view:	top level	**Lines:**	3270	7970	41.0 %
Test:	id:002084,src:002034,op:havoc,rep:2.lcov_info_final	**Functions:**	224	390	57.4 %
Date:	2015-05-25	**Branches:**	1778	5269	33.7 %

Directory	Line Coverage		Functions		Branches	
server	28.4 %	876 / 3080	39.5 %	49 / 124	27.0 %	541 / 2007
client	33.8 %	690 / 2039	54.9 %	39 / 71	31.5 %	397 / 1260
lib	59.8 %	1704 / 2851	69.7 %	136 / 195	42.0 %	840 / 2002

Generated by: LCOV version 1.10

Visualization of afl-cov[2]

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. “afl-cov - AFL Fuzzing Code Coverage”, Rash

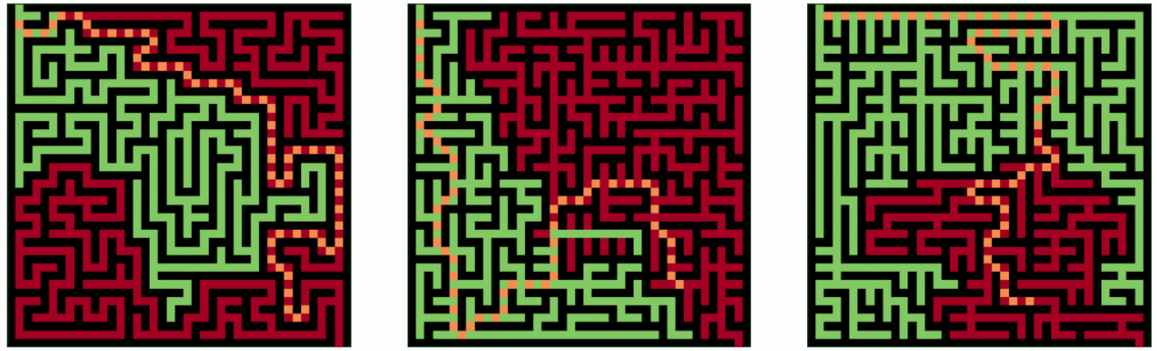
Challenge

Grey-box fuzzer is a black box

- Too many inputs to keep track of
- Beyond the scope of manual inspection
- Analysis is limited to the overall performance

Visualization Tools

- Focused on coverage analysis
- Insufficient for directed setting



Visualization of Fuzzle[1]

LCOV - code coverage report

			Hit	Total	Coverage
Current view:	top level	**Lines:**	3270	7970	41.0 %
Test:	id:002084,src:002034,op:havoc,rep:2.lcov_info_final	**Functions:**	224	390	57.4 %
Date:	2015-05-25	**Branches:**	1778	5269	33.7 %

Directory	Line Coverage		Functions		Branches	
server	28.4 %	876 / 3080	39.5 %	49 / 124	27.0 %	541 / 2007
client	33.8 %	690 / 2039	54.9 %	39 / 71	31.5 %	397 / 1260
lib	59.8 %	1704 / 2851	69.7 %	136 / 195	42.0 %	840 / 2002

Generated by: LCOV version 1.10

Visualization of afl-cov[2]

1. "Fuzzle: Making a Puzzle for Fuzzers", Lee, Kim, and Cha, ASE 2022
2. “afl-cov - AFL Fuzzing Code Coverage”, Rash

Our Solution

Our Solution

GeneVis: Genealogical Visualization Tool

Our Solution

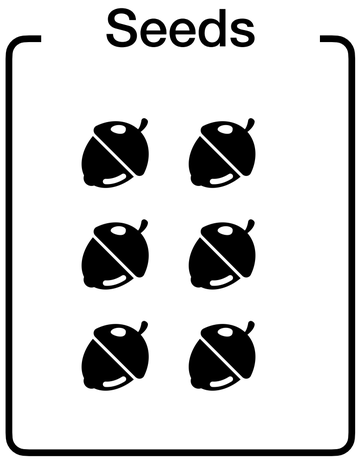
GeneVis: Genealogical Visualization Tool

- Tree structure based on the relationship between inputs

Our Solution

GeneVis: Genealogical Visualization Tool

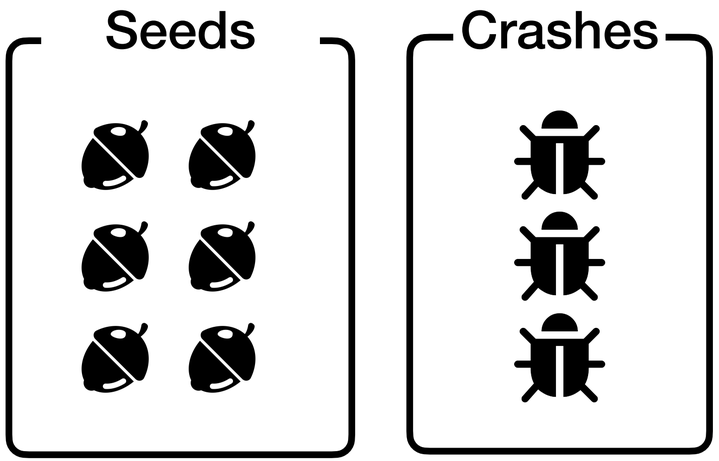
- Tree structure based on the relationship between inputs



Our Solution

GeneVis: Genealogical Visualization Tool

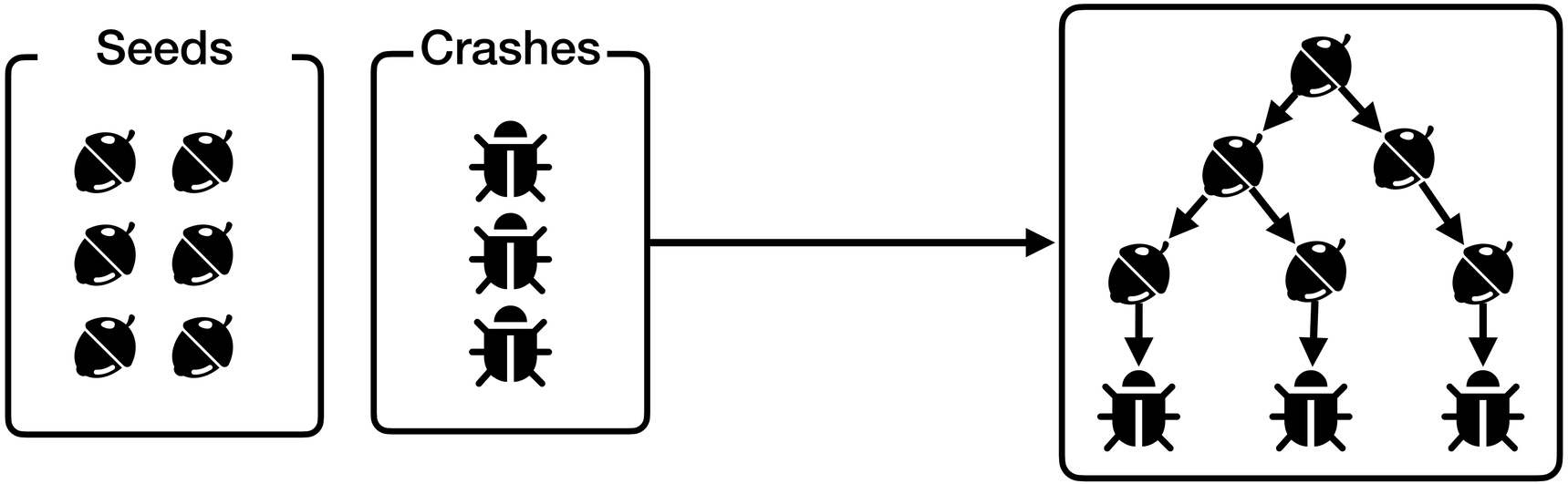
- Tree structure based on the relationship between inputs



Our Solution

GeneVis: Genealogical Visualization Tool

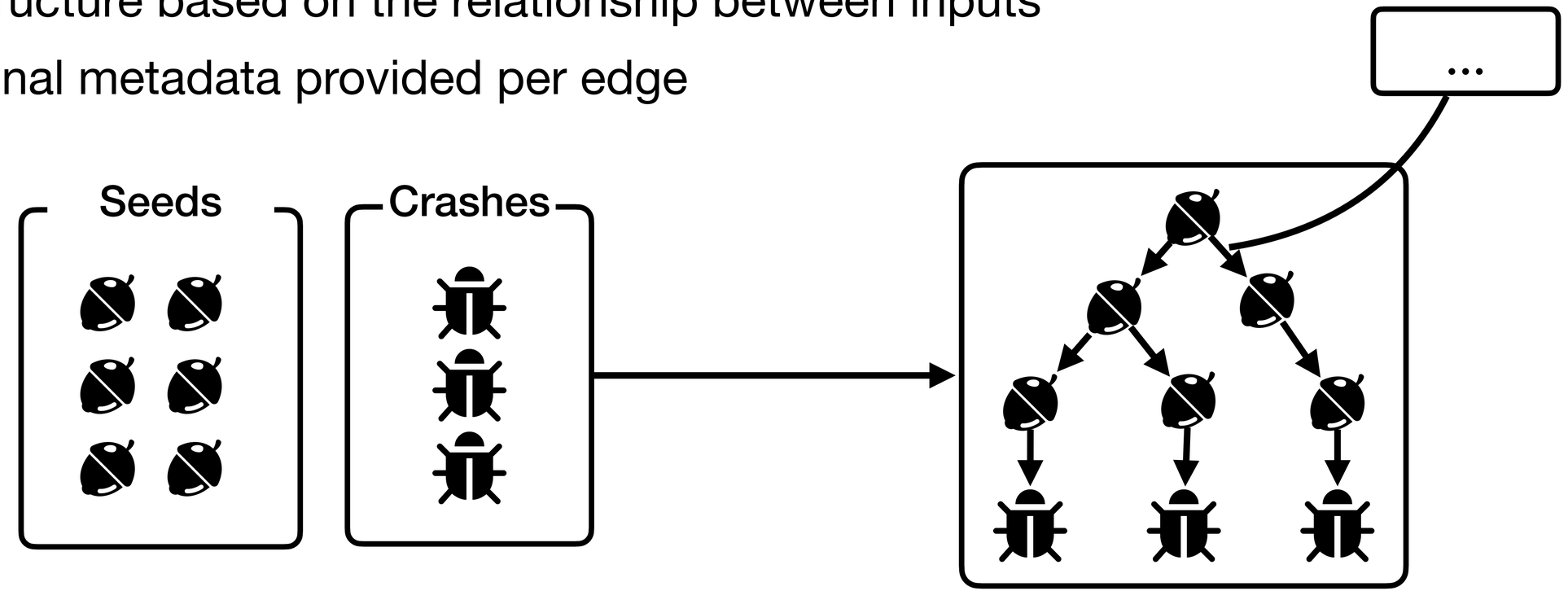
- Tree structure based on the relationship between inputs



Our Solution

GeneVis: Genealogical Visualization Tool

- Tree structure based on the relationship between inputs
- Additional metadata provided per edge



Demo

Demo

Features

Demo

Features

- Structural

Demo

Features

- Structural
  - Parent-Child relationship

Demo

Features

- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed

Demo

Features

- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed

- Metadata

Demo

Features

- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed

- Metadata
  - Coverage information

Demo

Features

- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed

- Metadata
  - Coverage information
  - Temporal information

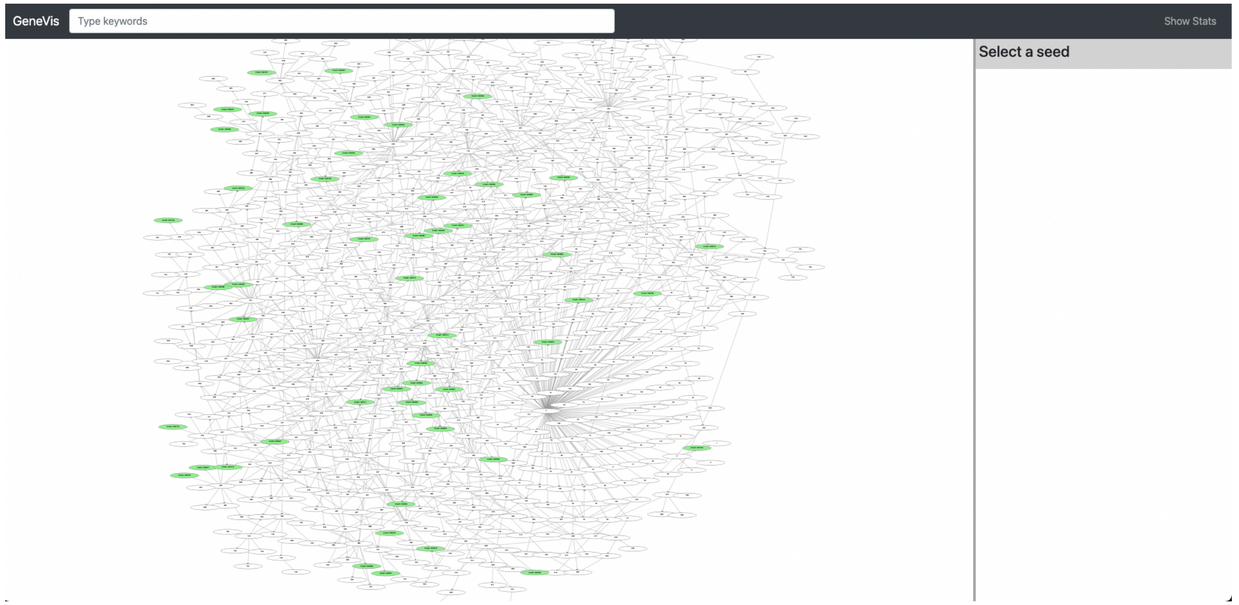
Demo

Features

- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed

- Metadata
  - Coverage information
  - Temporal information
  - Mutation information

Demo



http://elvis08.kaist.ac.kr/goodtaeeun/genevis/demo1/

Features

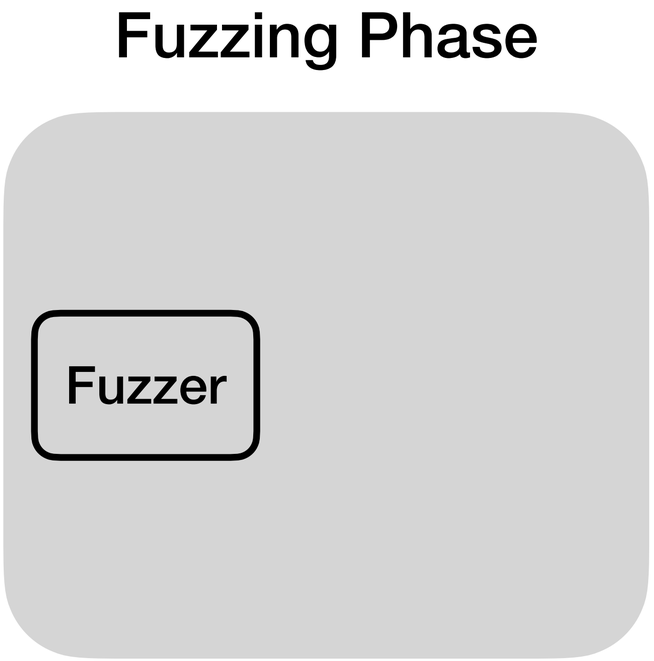
- Structural
  - Parent-Child relationship
  - Direct relationship with the initial seed
- Metadata
  - Coverage information
  - Temporal information
  - Mutation information

Overview

Overview

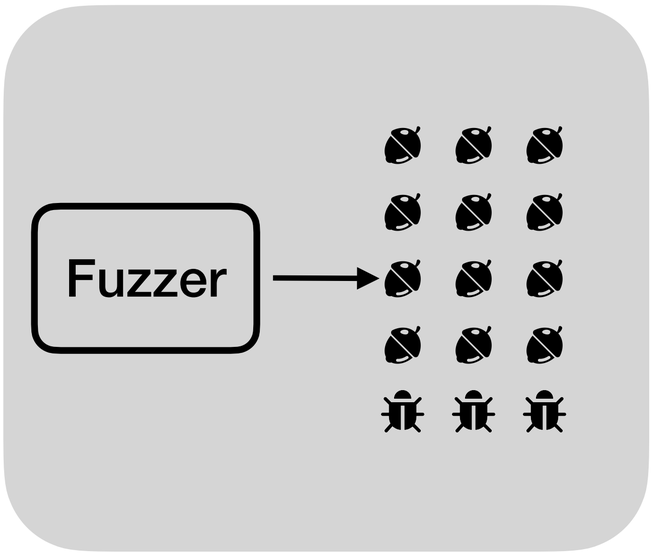
Fuzzing Phase

Overview

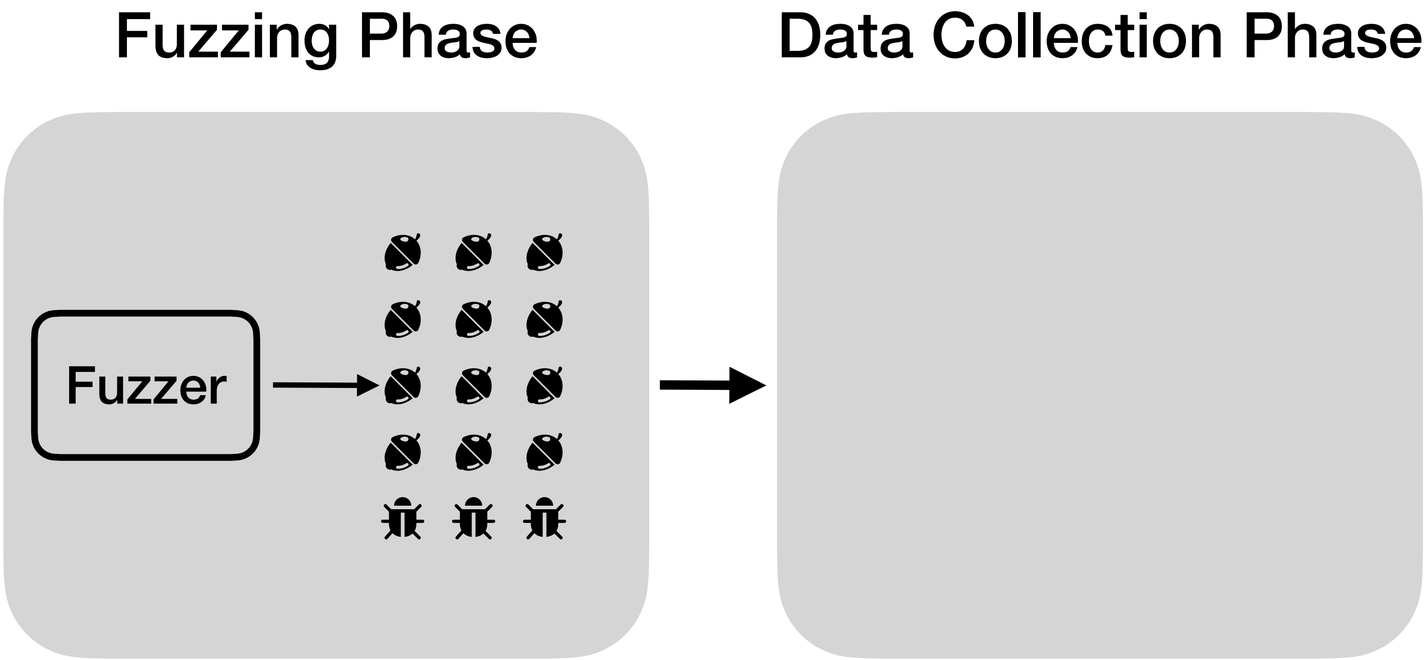


Overview

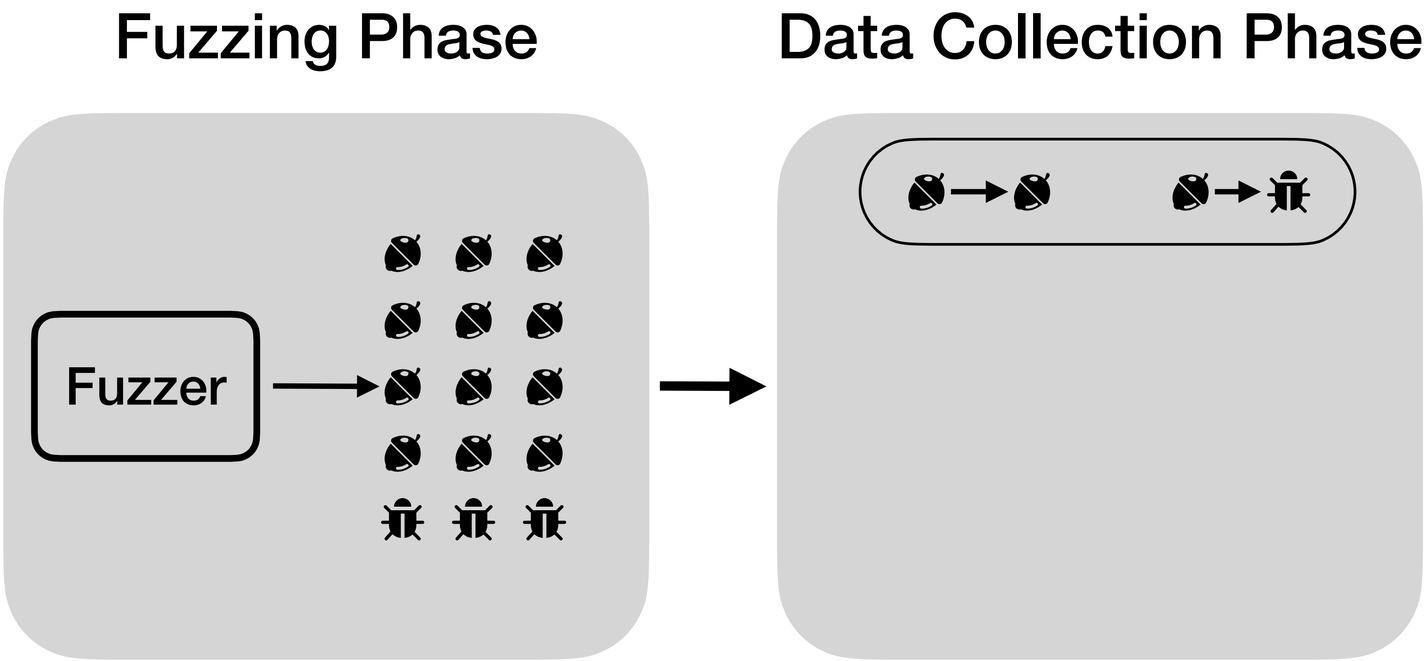
Fuzzing Phase



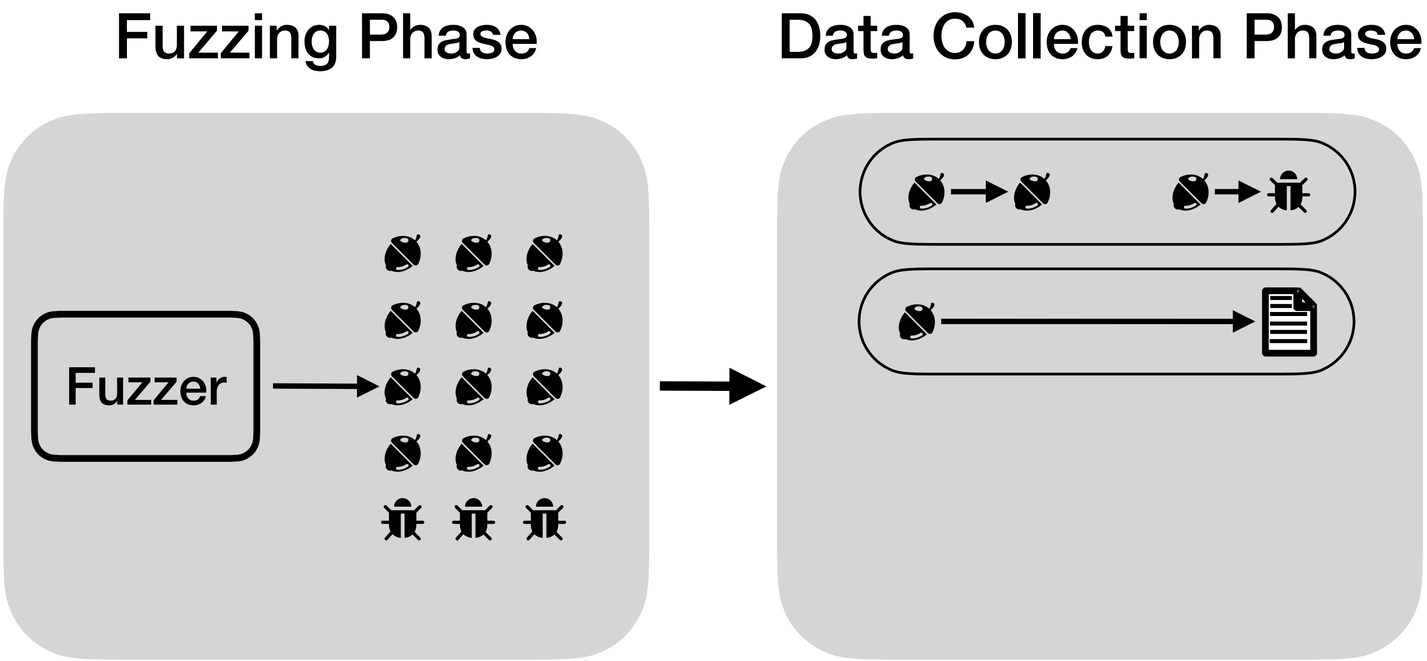
Overview



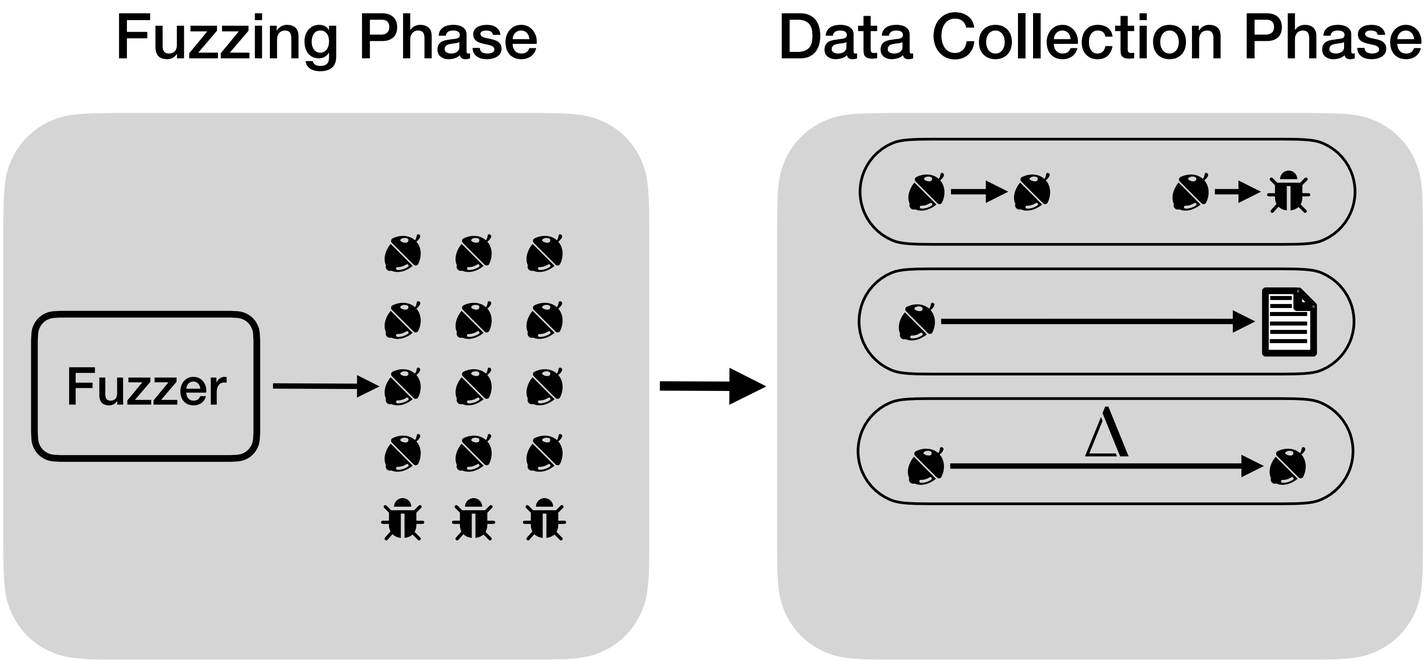
Overview



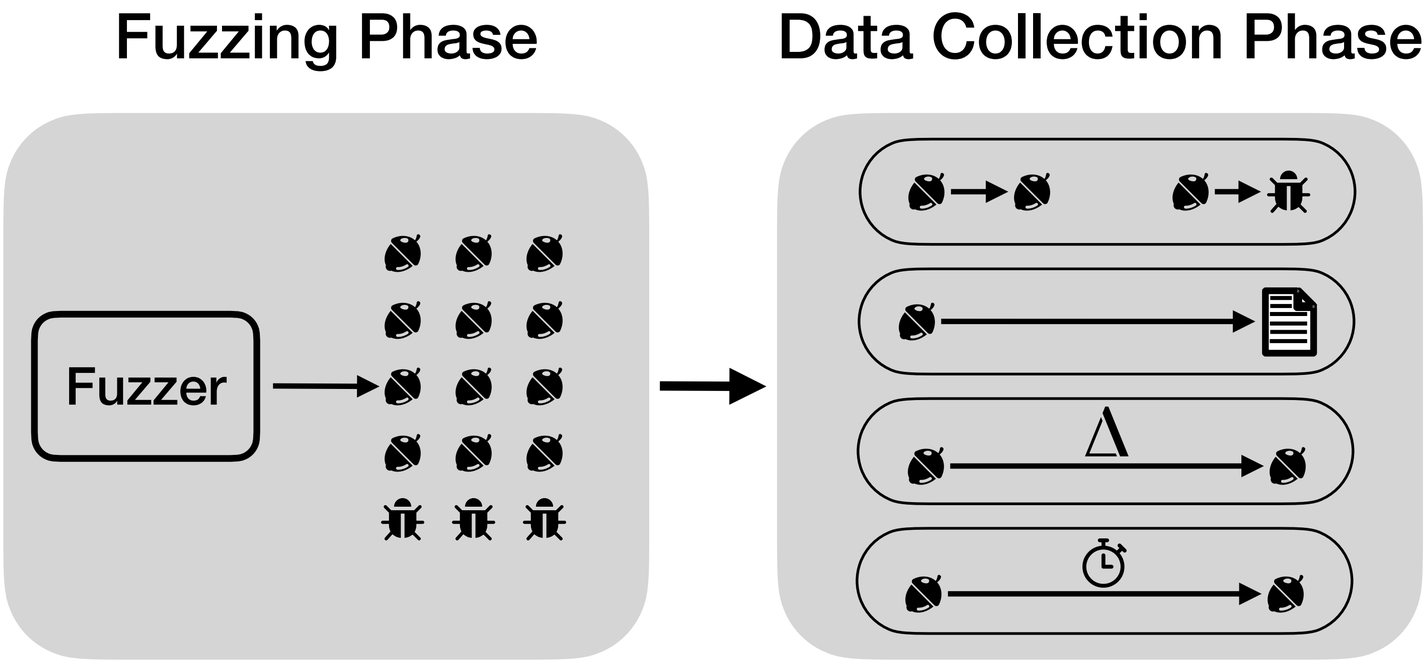
Overview



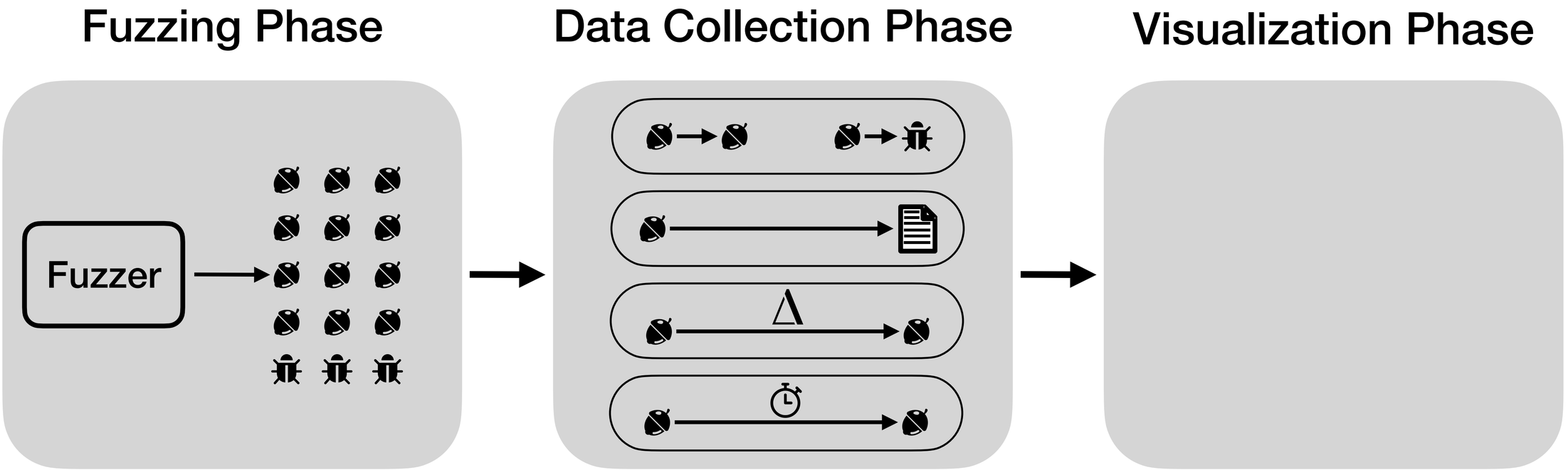
Overview



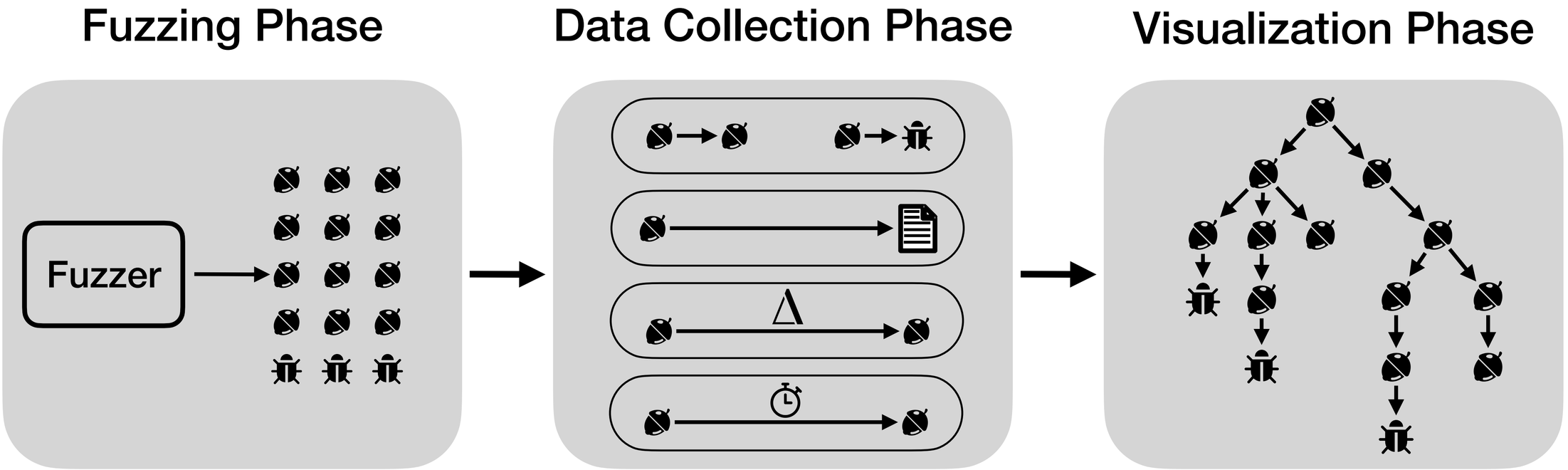
Overview



Overview


Fuzzing Phase
Data Collection Phase
Visualization Phase
Fuzzer

Overview


Fuzzing Phase
Data Collection Phase
Visualization Phase
Fuzzer
Δ

Key Challenges

Key Challenges

Data Collection

Key Challenges

Data Collection

- Structure of genealogical tree

Key Challenges

Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis

Key Challenges

Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

Key Challenges

Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

Visualization

Key Challenges

Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

Visualization

- Graphical visualization of collected data

Key Challenges

Data Collection

- Structure of genealogical tree
- Metadata to enhance analysis
- Must be **compatible**

Visualization

- Graphical visualization of collected data
- Must be **scalable** and **interactive**

Data Collection

Data Collection

Objectives

Data Collection

Objectives

- Structure of the genealogical tree

Data Collection

Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs

Data Collection

Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata

Data Collection

Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?

Data Collection

Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?
  - **How** was the progress made?

Data Collection

Objectives

- Structure of the genealogical tree
  - **Parent-child** relationships between inputs
- Other metadata
  - **What** was the progress?
  - **How** was the progress made?
  - How **difficult** was the progress?

Data Collection

Parent-child relationships between inputs

Data Collection

Parent-child relationships between inputs

- Naming convention of AFL

Data Collection

Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,src:000021,op:havoc,rep:2”

Data Collection

Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent

Data Collection

Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent

Data Collection

Parent-child relationships between inputs

- Naming convention of AFL
  - “id:000027,src:000021,op:havoc,rep:2”
  - Input “000027” has input “000021” as a parent

- Compatible with 11 out of 14 state-of-the-art Directed Grey-box Fuzzers

Data Collection

Metadata per edge

Data Collection

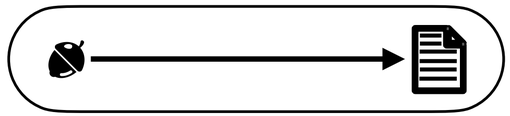
Metadata per edge

- **What** was the progress?

Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage



Collecting Coverage

Collecting Coverage

Visualization for Directed Fuzzing

Collecting Coverage

Visualization for Directed Fuzzing

- Not all coverage matters

Collecting Coverage

Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Collecting Coverage

Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Coverage with respect to the target

Collecting Coverage

Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Coverage with respect to the target

- Target function reachability

Collecting Coverage

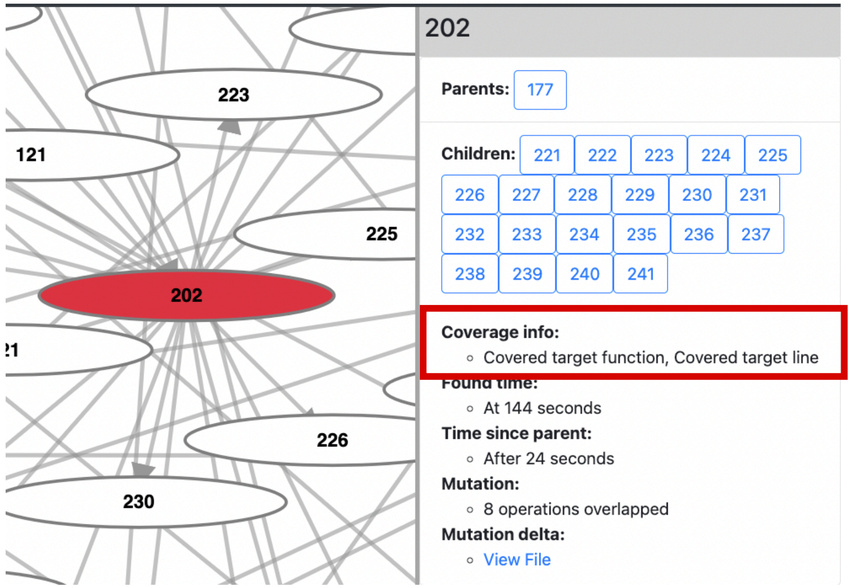
Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Coverage with respect to the target

- Target function reachability
- Target line reachability

Collecting Coverage



Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Coverage with respect to the target

- Target function reachability
- Target line reachability

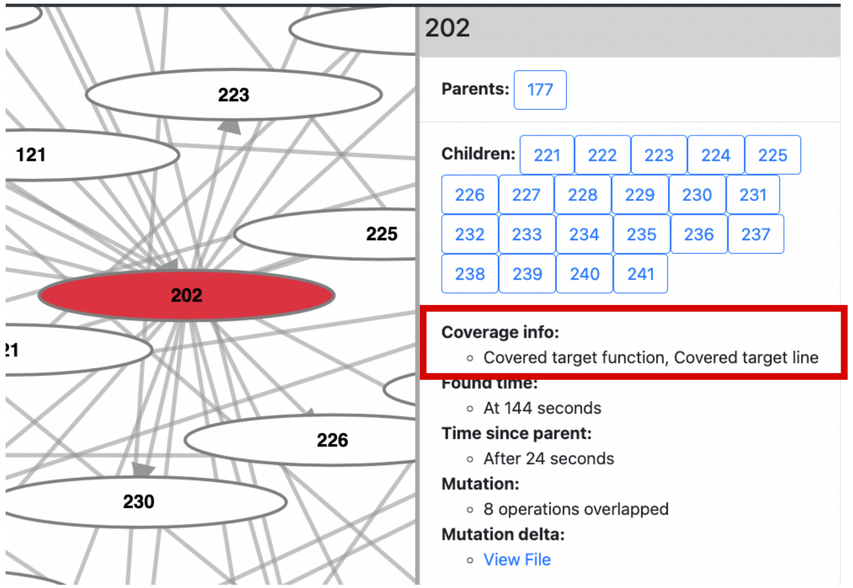
Collecting Coverage

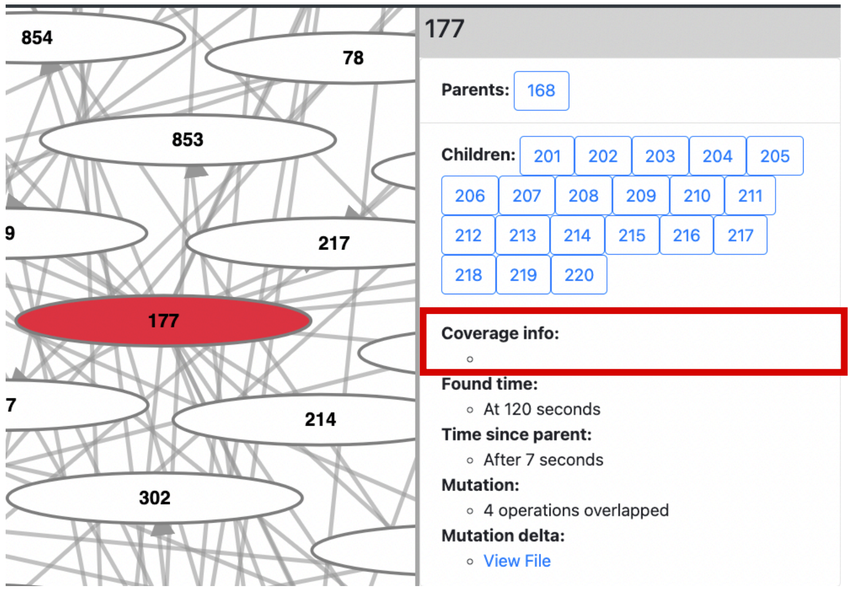
Visualization for Directed Fuzzing

- Not all coverage matters
- Not all seeds cover new lines

Coverage with respect to the target

- Target function reachability
- Target line reachability





Collecting Coverage

Visualization for Directed Fuzzing

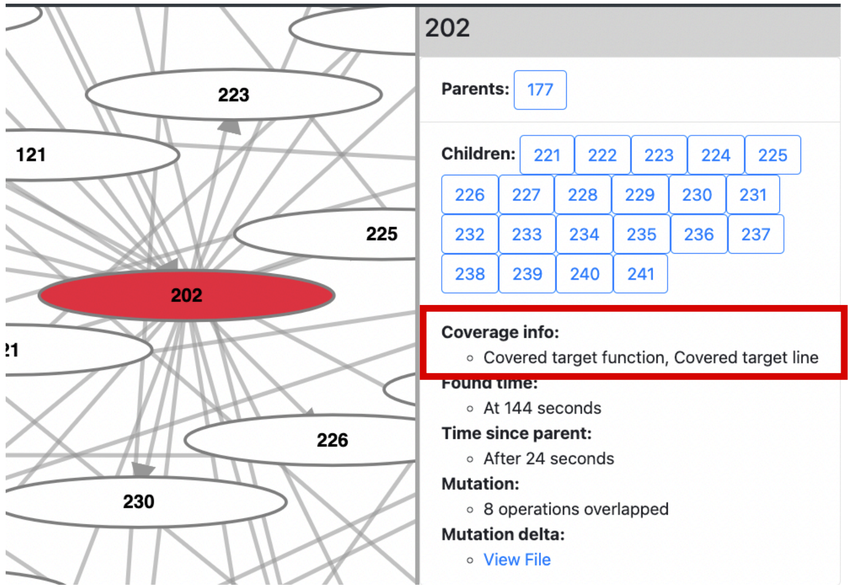
- Not all coverage matters
- Not all seeds cover new lines

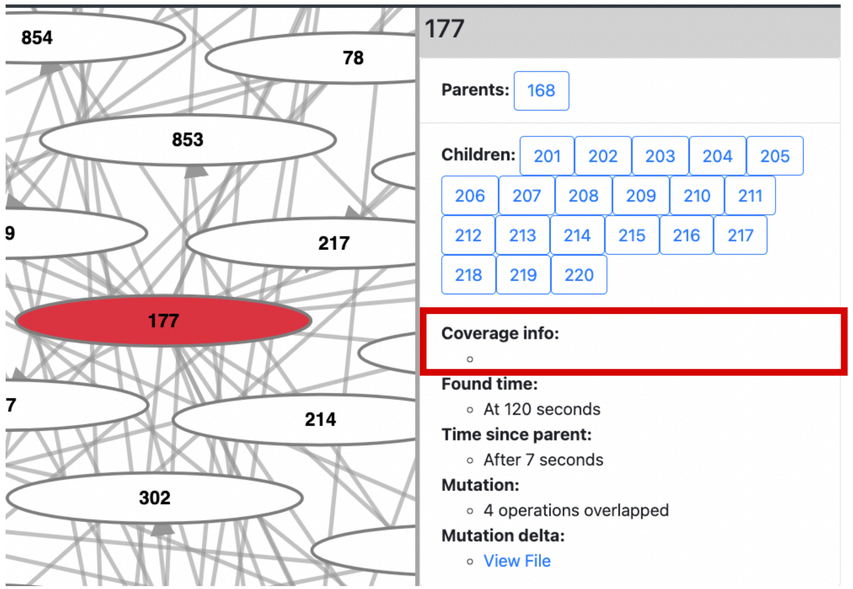
Coverage with respect to the target

- Target function reachability
- Target line reachability

Instrumented binary

- Instrumented with LLVM compiler pass

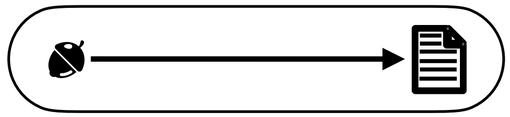




Data Collection

Metadata per edge

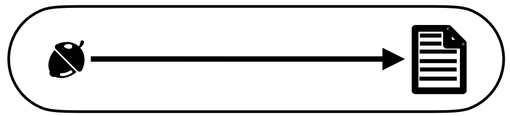
- **What** was the progress?
  - Coverage of target function/line



Data Collection

Metadata per edge

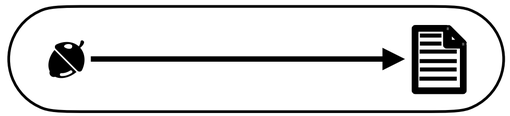
- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?

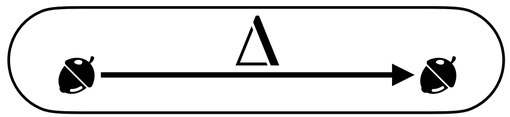


Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs





Collecting Mutation information

Mutation Information

Collecting Mutation information

Mutation Information

- The intensity of the mutation: # of applied mutations

Collecting Mutation information

Mutation Information

- The intensity of the mutation: # of applied mutations
- Diff between parent and child seeds

Collecting Mutation information

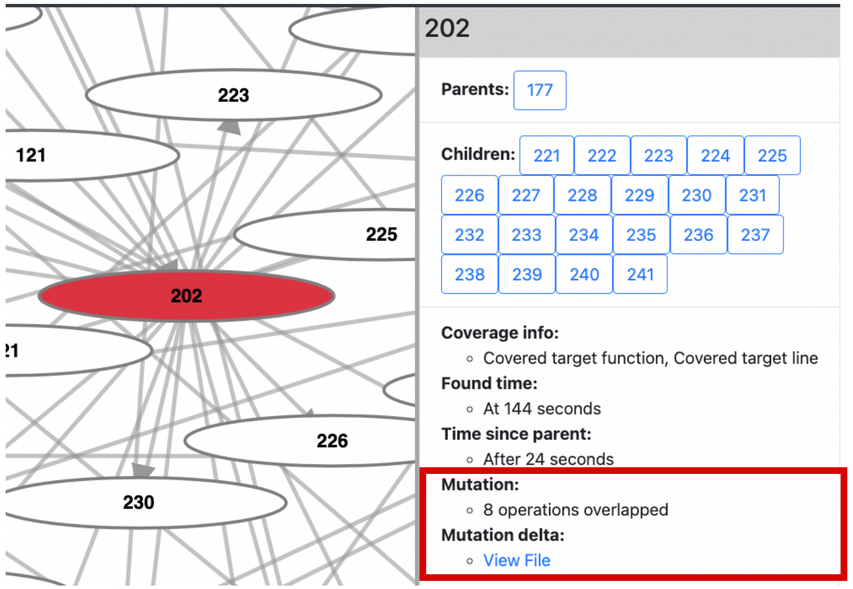
Mutation Information

- The intensity of the mutation: # of applied mutations
- Diff between parent and child seeds
  - Too large, thus provided as a link to a file

Collecting Mutation information

Mutation Information

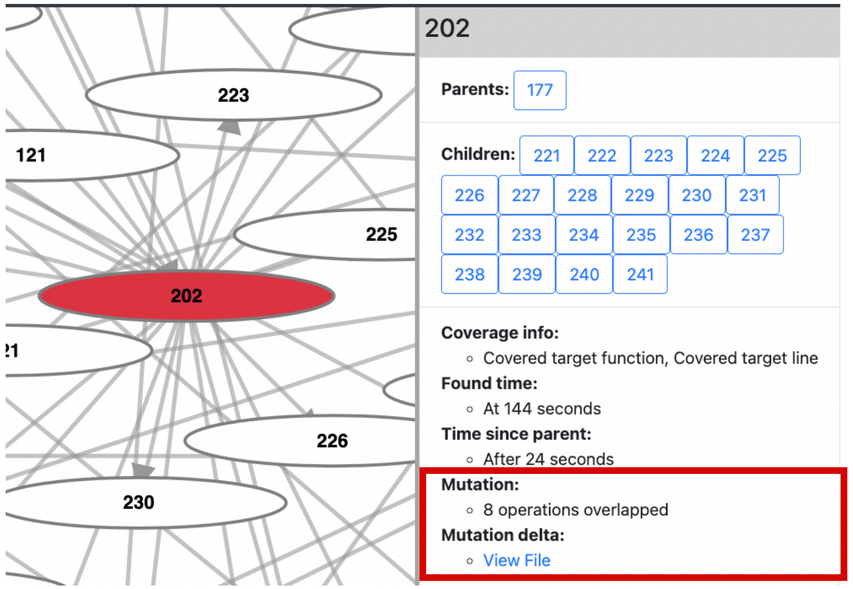
- The intensity of the mutation: # of applied mutations
- Diff between parent and child seeds
  - Too large, thus provided as a link to a file



Collecting Mutation information

Mutation Information

- The intensity of the mutation: # of applied mutations
- Diff between parent and child seeds
  - Too large, thus provided as a link to a file

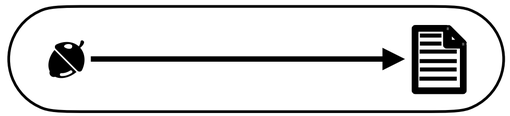


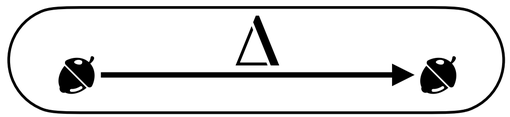

```
---
+++
@@ -43,8 +43,8 @@
  28
  f6
  02
-00 20
+a6 ab
  4e
  f8
  93
@@ -251,7 +251,7 @@
  03
  12
  34
-4d
+40
  34
  56
  00
```

Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs

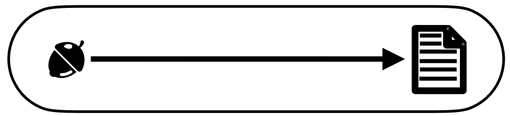


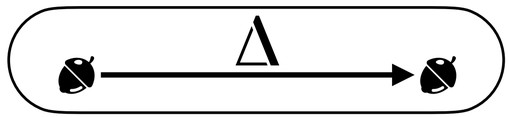


Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?

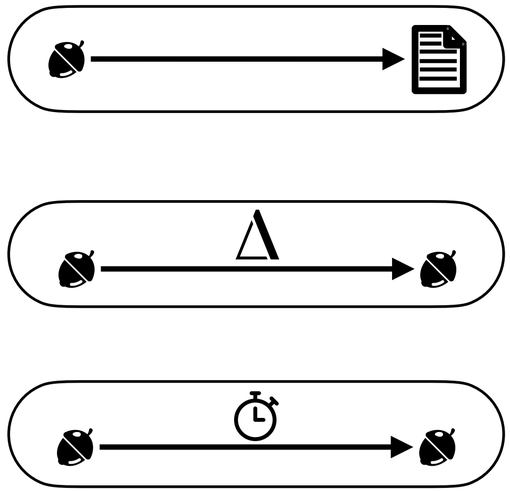




Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?
  - Generation time delta between parent-child inputs



Collecting Time Log

Collecting Time Log

Post-process the generated inputs

Collecting Time Log

Post-process the generated inputs

- After fuzzing, inspect the output directory

Collecting Time Log

Post-process the generated inputs

- After fuzzing, inspect the output directory

Absolute & Relative time information

Collecting Time Log

Post-process the generated inputs

- After fuzzing, inspect the output directory

Absolute & Relative time information

- Found time

Collecting Time Log

Post-process the generated inputs

- After fuzzing, inspect the output directory

Absolute & Relative time information

- Found time
- Time since parent was found

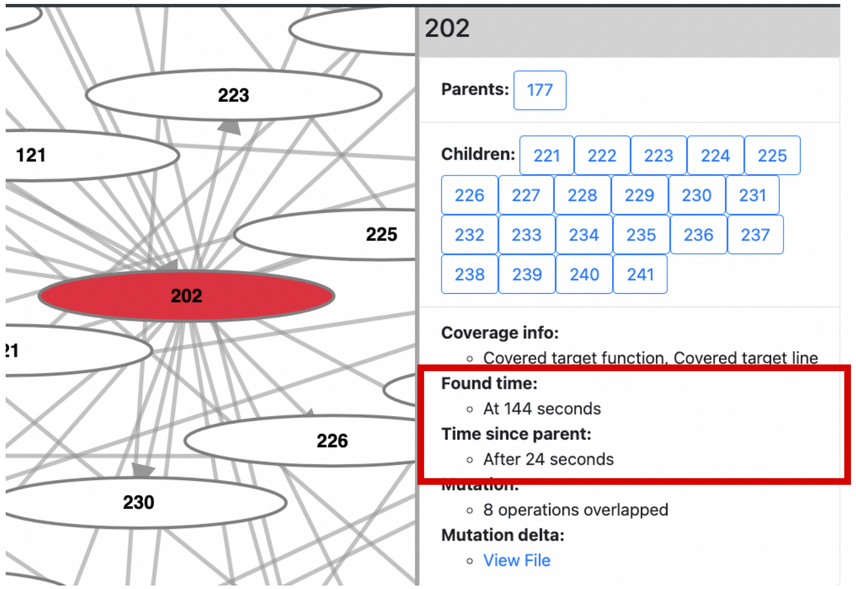
Collecting Time Log

Post-process the generated inputs

- After fuzzing, inspect the output directory

Absolute & Relative time information

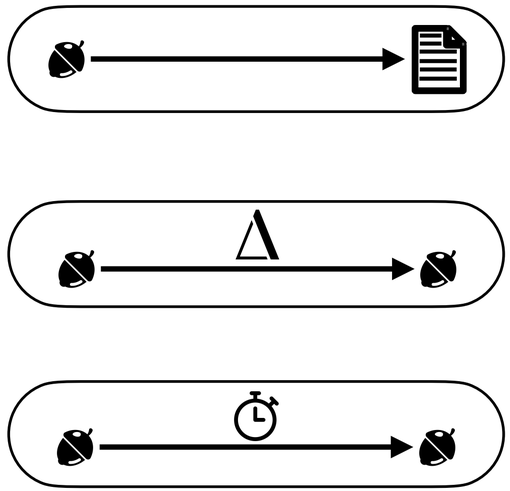
- Found time
- Time since parent was found



Data Collection

Metadata per edge

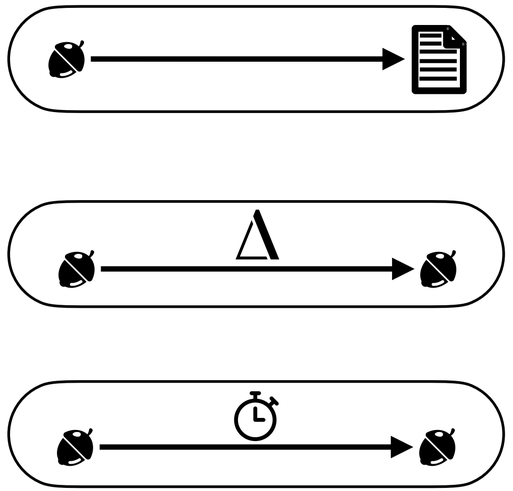
- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?
  - Generation time delta between parent-child inputs



Data Collection

Metadata per edge

- **What** was the progress?
  - Coverage of target function/line
- **How** was the progress made?
  - Mutation delta between parent-child inputs
- How **difficult** was the progress?
  - Generation time delta between parent-child inputs



- Independent from fuzzer implementation

Visualization

Visualization

D3: Data visualization library

Visualization

D3: Data visualization library

- **Scalable**

Visualization

D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format

Visualization

D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss

Visualization

D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**

Visualization

D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**
  - Supports various interactions

Visualization

D3: Data visualization library

- **Scalable**
  - Generates graph in SVG format
  - Supports large-scale images with no resolution loss
- **Interactive**
  - Supports various interactions
  - Zoom in/out, toggle, traversing the graph

Implementation

- **Coverage Instrumentation**
  - LLVM compiler pass

- **Data Parsing**
  - Python and Bash script

- **Visualization**
  - JavaScript, D3 library

Results

Results

GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers

Results

GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers

Results

GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data (less than 1 minute to generate)

Results

GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers

- **Compatible** with 11 state-of-the-art Directed Grey-box Fuzzers
- **Scalable** to large-scale data (less than 1 minute to generate)
- **Interactive** to provide zoom in/out, toggle, traversing the graph

Future Works

Future Works

Coverage Information

Future Works

Coverage Information

- More fine-grained coverage information

Future Works

Coverage Information

- More fine-grained coverage information

Mutation Information

Future Works

Coverage Information

- More fine-grained coverage information

Mutation Information

- Identify the critical part of the mutation that caused the progress

Future Works

Coverage Information

- More fine-grained coverage information

Mutation Information

- Identify the critical part of the mutation that caused the progress
- Connect mutation to the impacted program location

Summary

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive

- **Contributions**

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive

- **Contributions**
  - Enable precise analysis of the performance of Directed Grey-box Fuzzing

Summary

- **Challenges in analyzing Directed Grey-box Fuzzing**
  - The number of inputs does not scale
  - Grey-box fuzzer is black-box to users

- **GeneVis: Genealogical Visualization Tool for Directed Grey-box Fuzzers**
  - Compatible
  - Scalable
  - Interactive

- **Contributions**
  - Enable precise analysis of the performance of Directed Grey-box Fuzzing
  - Open up the opportunity to further improve the field of Directed Grey-box Fuzzing