Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Obfuscating Transformations

Yury Lifshits

Mathematics & Mechanics Faculty Saint Petersburg State University

Spring 2005 - SETLab

Outline

Obfuscating Transformations

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator
- Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness Further Research

Summary

1 What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator
- Obfuscator Characteristics

Outline

Obfuscating Transformations

Yury Lifshits

1

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator
- Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator
- Obfuscator Characteristics

2 Library of Obfuscating Transformations

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Outline

Obfuscating Transformations

Yury Lifshits

1

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator
- Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator
- Obfuscator Characteristics

2 Library of Obfuscating Transformations

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

3 Obfuscation vs. Deobfuscation

- Classical Program Analysis
- Deobfuscation Hardness
- Further Research

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator

Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Motivation: Java Virtual Machine

What is difference between Java and others?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Motivation: Java Virtual Machine

What is difference between Java and others?

Most programming languages:

Source Code ↓ Machine Code ↓ Predefined Architecture

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What is difference between Java and others?

Most programming languages:	Java:
Source Code \downarrow	Java Source Code
Machine Code ↓	Java-byte Code ↓
Predefined	Virtual Processor = JVM
Architecture	OS & Hardware

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Motivation: Java Virtual Machine

What is difference between Java and others?



Java Virtual Machine: implemented on huge number of hardware architectures / operating systems

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Notion of Obfuscator

Objectives:

⇒ Make code not readable by human

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Objectives:

- ⇒ Make code not readable by human
- ⇒ Make automated analysis difficult

Notion of Obfuscator

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Objectives:

- ⇒ Make code not readable by human
- ⇒ Make automated analysis difficult
- ⇒ Make code more complicated

Notion of Obfuscator

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Objectives:

- ⇒ Make code not readable by human
- ⇒ Make automated analysis difficult
- ⇒ Make code more complicated
- ⇒ Make decompilation & reverse engineering difficult

Notion of Obfuscator

Anatomy of Obfuscator I

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

How real obfuscator works?

Anatomy of Obfuscator I

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How real obfuscator works?

1 Prepares program to be obfuscated

Anatomy of Obfuscator I

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How real obfuscator works?

Prepares program to be obfuscated

2 Makes a single transformation

Anatomy of Obfuscator I

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How real obfuscator works?

- Prepares program to be obfuscated
- 2 Makes a single transformation
- 3 Repeats step 2 until task completed or constraints exceeded

Anatomy of Obfuscator II

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

How real obfuscator works (more precisely)?

Anatomy of Obfuscator II

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

How real obfuscator works (more precisely)?

The workflow is:

⇒ Parse input program

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- → Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)
 - Makes some appropriateness suggestions

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)
 - Makes some appropriateness suggestions
- Main while loop (until constraints are exceeded or quality is achieved)

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)
 - Makes some appropriateness suggestions
- Main while loop (until constraints are exceeded or quality is achieved)
 - Choose next (by priority) element of the program to be obfuscated

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)
 - Makes some appropriateness suggestions
- Main while loop (until constraints are exceeded or quality is achieved)
 - Choose next (by priority) element of the program to be obfuscated
 - Implement appropriate obfuscating transformation (from obfuscator library)

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator
- Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Anatomy of Obfuscator II

How real obfuscator works (more precisely)?

- ⇒ Parse input program
 - Makes a list of obfuscation candidates: classes, variables, methods
 - Constructs internal representation of the program (e.g. control flow and basic blocks)
 - Makes some appropriateness suggestions
- Main while loop (until constraints are exceeded or quality is achieved)
 - Choose next (by priority) element of the program to be obfuscated
 - Implement appropriate obfuscating transformation (from obfuscator library)
 - Update internal representation

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Quality of Obfuscation

Slide from Lecture 1

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Quality of Obfuscation

Slide from Lecture 1

So you supposed to explain it to me...

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Slide from Lecture 1

So you supposed to explain it to me...

Strength can be measured by:

- \Rightarrow Potency
 - $\frac{E(P')}{E(P)} 1$
- ⇒ Resilience

Trivial, weak, strong, full, one-way

⇒ Cost

Free, cheap, costly, expensive

⇒ Stealthy

Quality of Obfuscation

Program Complexity Metrics

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

We want: make program complicated

Program Complexity Metrics

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

We want: make program complicated

So what is program code complexity?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Number of operators and operands

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

We want: make program complicated

So what is program code complexity?

Program Complexity Metrics

Program length

Number of operators and operands

⇒ Data flow complexity

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

⇒ Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

→ Cyclomatic complexity

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

⇒ Cyclomatic complexity

Number of predicates in a function
Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

⇒ Program length

 \Box

Number of operators and operands

Number of inter-block variable references

⇒ Cyclomatic complexity

Data flow complexity

Number of predicates in a function

⇒ Nesting complexity

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

⇒ Program length

Number of operators and operands

 \Rightarrow Data flow complexity

Number of inter-block variable references

⇒ Cyclomatic complexity

Number of predicates in a function

Nesting complexity

Number of nesting level of conditionals in a program

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

⇒ Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

⇒ Cyclomatic complexity

Number of predicates in a function

⇒ Nesting complexity

Number of nesting level of conditionals in a program

Data structure complexity

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

⇒ Program length

Number of operators and operands

 \Rightarrow Data flow complexity

Number of inter-block variable references

→ Cyclomatic complexity

Number of predicates in a function

⇒ Nesting complexity

Number of nesting level of conditionals in a program

Data structure complexity

Complexity of the static data structures in the program like variables, vectors, records

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

→ Cyclomatic complexity

Number of predicates in a function

Nesting complexity

Number of nesting level of conditionals in a program

⇒ Data structure complexity

Complexity of the static data structures in the program like variables, vectors, records

⇒ OO Metrics

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Program Complexity Metrics

We want: make program complicated

So what is program code complexity?

Program length

Number of operators and operands

⇒ Data flow complexity

Number of inter-block variable references

→ Cyclomatic complexity

Number of predicates in a function

⇒ Nesting complexity

Number of nesting level of conditionals in a program

Data structure complexity

Complexity of the static data structures in the program like variables, vectors, records

⇒ OO Metrics

Level of inheritance, coupling, number of methods triggered by another method, non-cohesiveness

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

What do we pay for security?

Cost Analysis

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

What do we pay for security?

Costs at creation time

Obfuscation need time!

Cost Analysis

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What do we pay for security?

Costs at creation time

Obfuscation need time!

Cost Analysis

Costs at transmition time (resulting size) Inlining library functions may increase size enormously!

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What do we pay for security?

Costs at creation time

Obfuscation need time!

- Costs at transmition time (resulting size) Inlining library functions may increase size enormously!
- Cost at execution time

Checking procedures, dummy code, inlining

Cost Analysis

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

 \Box

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What do we pay for security?

Costs at creation time

Obfuscation need time!

Cost Analysis

→ Costs at transmition time (resulting size)

Inlining library functions may increase size enormously!

Cost at execution time

Checking procedures, dummy code, inlining Cost by not using efficiency enhancing mechanisms Caching is rarely possible; losing module structure

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

Other metrics?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Statistics measurement

Other metrics?

Statistics! What kind of?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Statistics measurement

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

Use rare elements more often

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

- Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

- Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!
 - Usage of variables

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

- Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!
 - Usage of variables
 - Data processing

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

⇒ Distribution of basic constructions

- Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!
 - Usage of variables
 - Data processing
 - Control flow commands

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

- ⇒ Distribution of basic constructions
 - Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!
 - Usage of variables
 - Data processing
 - Control flow commands
- ⇒ Code patterns

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Other metrics?

Statistics! What kind of?

- ⇒ Distribution of basic constructions
 - Use rare elements more often
- Clustering of program elements. Uniform distribution difficult to understand!
 - Usage of variables
 - Data processing
 - Control flow commands
- ⇒ Code patterns
 - Destroy long patterns in program

Obfuscating \$ ='ev Transformaal(seek\040D tions ATA.0. 0:•):foreach(1..3) {<DATA>:}mv @camel1hump:mv\$camel; Yury Lifshits mv#Camel :while(<DATA>) (\$ =sprintf("%-6 9s•,\$_);my@dromedarv 1=split(//); if (defined (# =<DATA>)) (@camel1hum p=split(//);}while(@dromeda What is rv1) {mvscamel1hump=0 ;my#CAHEL=3;if(defined(#_=shif **Obfuscator?** t (@dromedarv1)) & & /\S/) {\$ camel1hump+=1<<\$ CANEL; } \$CAHEL - - ; if (d Notion of efined (# =shift(@dromedarv1))&&/\S/) { Obfuscator \$camel1hump+=1 <<\$CAHEL: } \$CAHEL- : if (defined (\$ =shift(Anatomy of @camel1hump))&&/\\$/) {\$camel1hump+=1<<\$CAHEL:}\$CAHEL::if(</pre> Obfuscator defined (\$ =shift (@camel1hump)) &&/\S/) {\$camel1hump+=1<<\$CAHE L::}\$camel.=(split(//.*\040..m^{/J\047\134}L^7FX*)) [\$camel1h Obfuscator Characteristics ump];}\$camel.='\n';}@camel1hump=split(/\n/,\$camel);foreach(@ camel1hump) {chomp; \$Camel=\$; y/LJF7\173\175 \047/\061\062\063\ Obfuscation 064\065\066\067\070/;y/12345678/JL7F\175\173\047'/;\$ =reverse; Library print \$ \040\$Camel\n"; } foreach (@camel1hump) {chomp; \$Camel=\$;y Program /LJF7\173\175`\047/12345678/;y/12345678/JL7F\175\173\0 47'/; Representation \$ =reverse:print!\040\$ \$Camel\n!:}'::s/\s*//g::eval: eval (*seek\040DATA,0,0;*);undef\$/;\$ =<DATA>;s/\s*//q;():::8 Data & Control · Basic Tricks ;^.* ;;;map{eval*print*\$ **;}/.{4}/q; DATA \124 50\145\040\165\163\145\040\157\1 46\040\1 41\0 Control Flow \1 Obfuscation 40\143\141 \155\145\1 54\040\1 51\155\ 141 Even more \147\145\0 40\151\156 \040\141 \163\16 3\ transformations 157\143\ 151\141\16 4\151\1 57\156 \040\167 \151\164\1 50\040\ $120 \ 1$ Obfuscation 45\162\ 154\040\15 1\163\ 040\14 vs. Deobfus-1\040\1 64\162\1 41\144 \145\ cation 155\14 1\162\ 153\04 0\157 \146\ 040\11 7\047\ 122\1 Classical Program 45\15 Analysis 1\154\1 54\171 040\046\ 012\101\16 3\16 Deobfuscation Hardness 3\15 7\143\15 1\14 1\16 4\145\163 \054 Further Research \040 \111\156\14 3\056 \040\ 125\163\145\14 4\040\ Summarv 167\1 51\164\1 50\0 40\160\ 145\162 \155\151 \163\163 \151\1 57\156\056

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

What is *program* from our point of view?

Control Flow Model I

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Anatomy o Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What is program from our point of view?



Control Flow Model I

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator

Obfuscator

Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary



Control Flow Model II

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary



Compilers and program optimization theory represent programs by control flow graph (CFG)

⇒ Each node in the graph represents a basic block

Control Flow Model II

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Control Flow Model II



Compilers and program optimization theory represent programs by control flow graph (CFG)

- ⇒ Each node in the graph represents a basic block
- ⇒ Basic block: straight-line piece of code without any jumps or jump targets

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Compilers and program optimization theory represent programs by control flow graph (CFG)

- ⇒ Each node in the graph represents a basic block
- ⇒ Basic block: straight-line piece of code without any jumps or jump targets
- Directed edges are used to represent jumps in the control flow

Control Flow Model II

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Control Flow Model II



Compilers and program optimization theory represent programs by control flow graph (CFG)

- ⇒ Each node in the graph represents a basic block
- ⇒ Basic block: straight-line piece of code without any jumps or jump targets
- Directed edges are used to represent jumps in the control flow
- ⇒ Jump targets start a block; jumps end a block

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Simple transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator

Characteristics Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

So what transformations do you can suggest?

⇒ Data Obfuscation

Simple transformations

Yury Lifshits

Simple transformations

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

So what transformations do you can suggest?

Data Obfuscation

Variable splitting

Simple transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion

Simple transformations

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure

Simple transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator

Characteristics Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime

Simple transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator

Characteristics Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

So what transformations do you can suggest?

Data Obfuscation

- Variable splitting
- Scalar/object conversion
- Static data to procedure
- Change variable lifetime
- Split/fold/merge arrays
Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

So what transformations do you can suggest?

Data Obfuscation

- Variable splitting
- Scalar/object conversion
- Static data to procedure
- Change variable lifetime
- Split/fold/merge arrays
- Change encoding

Simple transformations

Simple transformations

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

So what transformations do you can suggest?

Data Obfuscation

- Variable splitting
- Scalar/object conversion
- Static data to procedure
- Change variable lifetime
- Split/fold/merge arrays
- Change encoding
- Merge scalar variables

Simple transformations

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

So what transformations do you can suggest?

Data Obfuscation

- Variable splitting
- Scalar/object conversion
- Static data to procedure
- Change variable lifetime
- Split/fold/merge arrays
- Change encoding
- Merge scalar variables

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

So what transformations do you can suggest?

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

Control Obfuscation

Simple transformations

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

So what transformations do you can suggest?

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

Control Obfuscation
Break basic blocks

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

So what transformations do you can suggest?

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

Control Obfuscation
Break basic blocks
Inline methods

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

- Control Obfuscation
 - Break basic blocks
 - Inline methods
 - Outline statements

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

- Control Obfuscation
 - Break basic blocks
 - Inline methods
 - Outline statements
 - Unroll loops

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

- Control Obfuscation
 - Break basic blocks
 - Inline methods
 - Outline statements
 - Unroll loops
 - Reorder statements

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Simple transformations

- Data Obfuscation
 - Variable splitting
 - Scalar/object conversion
 - Static data to procedure
 - Change variable lifetime
 - Split/fold/merge arrays
 - Change encoding
 - Merge scalar variables

- Control Obfuscation
 - Break basic blocks
 - Inline methods
 - Outline statements
 - Unroll loops
 - Reorder statements
 - Reorder loops

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation

Hardness

Further Research

Summary

Control Flow Flattening

How to destroy control flow graph?

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator
- Obfuscator
- Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How to destroy control flow graph?



Control Flow Flattening

Step by step:

⇒ Write down a list of all basic blocks

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

How to destroy control flow graph?



Step by step:

- ⇒ Write down a list of all basic blocks
- Split and merge some of them

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

How to destroy control flow graph?



Step by step:

- ⇒ Write down a list of all basic blocks
- Split and merge some of them
- Enumerate them

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Further Researc

Summary

How to destroy control flow graph?



Step by step:

- ⇒ Write down a list of all basic blocks
- Split and merge some of them
- Enumerate them
- ⇒ Replace all calls by indirect pointing

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator
- Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness Further Research
- Fulliel Researc
- Summary

How to destroy control flow graph?



Step by step:

- ⇒ Write down a list of all basic blocks
- Split and merge some of them
- Enumerate them
- ⇒ Replace all calls by indirect pointing
- ⇒ Write a single dispatcher to maintain all control flow

Opaque predicates

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator

Obfuscator Characteristics

Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation

Hardness

Further Research

Summary

How can we use IF operator for obfuscation?

Opaque predicates

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation

Hardness

Further Research

Summary

How can we use IF operator for obfuscation?



Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we use IF operator for obfuscation?



Opaque predicates: every time the same value Difficult to discover by automatical static analysis

Opaque predicates

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of

Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we use IF operator for obfuscation?



Opaque predicates: every time the same value Difficult to discover by automatical static analysis

Examples:

$$((q+q^2) \bmod 2) = 0$$

Opaque predicates

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we use IF operator for obfuscation?



Opaque predicates

Opaque predicates: every time the same value Difficult to discover by automatical static analysis

Examples:

$$((q+q^2) \bmod 2) = 0$$

 $mod 8) = 0 \text{ OR } ((q^3) mod 8)$

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

How can we make program procedures indistinguishable?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we make program procedures indistinguishable?

Procedures relations are expressed by Program Call Graph: procedures are nodes and procedure calls are directed edges

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we make program procedures indistinguishable?

- Procedures relations are expressed by Program Call Graph: procedures are nodes and procedure calls are directed edges
- Idea: merge functions and call universal function with additional parameter
- Difficulty: different signatures (input-output specifications)

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

How can we make program procedures indistinguishable?

Procedures relations are expressed by Program Call Graph: procedures are nodes and procedure calls are directed edges

Idea: merge functions and call universal function with additional parameter

Difficulty: different signatures (input-output specifications)

Solution: unify signatures (in groups)

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research
- Summary

Even more transformations

Question: Can you invent more?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Even more transformations

Question: Can you invent more?

⇒ Reuse identifiers

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Question: Can you invent more?

- ⇒ Reuse identifiers
- ⇒ Introduce misleading comments :-)

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Question: Can you invent more?

- ⇒ Reuse identifiers
- ⇒ Introduce misleading comments :-)
- ➡ Modify inheritance relations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Question: Can you invent more?

- Reuse identifiers
- ⇒ Introduce misleading comments :-)
- ⇒ Modify inheritance relations
- ⇒ Convert static data to procedural data

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Question: Can you invent more?

- Reuse identifiers
- ⇒ Introduce misleading comments :-)
- ⇒ Modify inheritance relations
- ⇒ Convert static data to procedural data
- Store part of the program as a text and interpret it only during runtime

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Question: Can you invent more?

- ⇒ Reuse identifiers
- ⇒ Introduce misleading comments :-)
- ⇒ Modify inheritance relations
- ⇒ Convert static data to procedural data
- Store part of the program as a text and interpret it only during runtime
- Remove library calls

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Advantages

Current Techniques: Pro and Contra

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Advantages

Easy to implement

- Universal
- Good against static analysis

Current Techniques: Pro and Contra

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Advantages

Easy to implement

Universal

 Good against static analysis

Current Techniques: Pro and Contra

Disadvantages

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Advantages

Easy to implement

- Universal
- Good against static analysis

Disadvantages

✗ No guaranteed security

Current Techniques: Pro and Contra
Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Advantages

Easy to implement

- Universal
- Good against static analysis

Disadvantages

- X No guaranteed security
- X Even no hope for that

Current Techniques: Pro and Contra

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Advantages

Easy to implement

- Universal
- Good against static analysis

Disadvantages

- X No guaranteed security
- X Even no hope for that
- Weak against dynamic attacks

Current Techniques: Pro and Contra

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator

Anatomy of Obfuscator

Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfus-

cation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Classical Program Analysis

What's about program analysis?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Classical Program Analysis

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Classical Program Analysis

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

⇒ May be aliased

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Classical Program Analysis

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- → Must be aliased

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- ⇒ Must be aliased
- ⇒ May be modified

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

- Deobfuscation Hardness
- Further Research

Summary

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- ⇒ Must be aliased
- ⇒ May be modified
- Must be constant

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness Further Research

Summary

Classical Program Analysis

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- Must be aliased
- ⇒ May be modified
- Must be constant
- Must be killed

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness Further Research

Summary

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- Must be aliased
- ⇒ May be modified
- Must be constant
- ⇒ Must be killed
- ⇒ Must be available

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis
- Deobfuscation Hardness Further Research
- Summary

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- Must be aliased
- ⇒ May be modified
- Must be constant
- ⇒ Must be killed
- ⇒ Must be available
- ⇒ May be used before kill

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis
- Deobfuscation Hardness Further Research
- Summary

What's about program analysis?

Static analysis: only read code Dynamic analysis: execute code

Usual tasks:

- ⇒ May be aliased
- Must be aliased
- May be modified
- Must be constant
- ⇒ Must be killed
- ⇒ Must be available
- ⇒ May be used before kill
- ⇒ May be referenced

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Is Deobfuscation Hard?

Can we prove the difficulty of deobfuscation?

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Is Deobfuscation Hard?

Can we prove the difficulty of deobfuscation?

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of
- Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Can we prove the difficulty of deobfuscation?

Not yet. But...

Is Deobfuscation Hard?

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Can we prove the difficulty of deobfuscation?

Not yet. But...

We can prove program analysis to be hard for obfuscated programs:

Is Deobfuscation Hard?

Yury Lifshits

What is Obfuscator?

- Notion of Obfuscator Anatomy of Obfuscator
- Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Can we prove the difficulty of deobfuscation?

Not yet. But...

We can prove program analysis to be hard for obfuscated programs:

Alias analysis of obfuscated programs is NP-hard!

Is Deobfuscation Hard?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis
- Deobfuscation Hardness
- Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

Deobfuscator can use:

⇒ Functions parameters catching

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

- ⇒ Functions parameters catching
- Program slicing

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

- ⇒ Functions parameters catching
- Program slicing
- Statistical analysis

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

- ⇒ Functions parameters catching
- Program slicing
- Statistical analysis
- ⇒ Data flow analysis

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow
- Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis

Deobfuscation Hardness

Further Research

Summary

Approaches to Deobfuscation

Almost all obfuscating transformations have a efficient deobfuscating method...

Do you believe?

- ⇒ Functions parameters catching
- Program slicing
- ⇒ Statistical analysis
- ⇒ Data flow analysis
- Pattern matching

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

- Program Representation
- Data & Control : Basic Tricks
- Control Flow Obfuscation
- Even more transformations

Obfuscation vs. Deobfuscation

- Classical Program Analysis Deobfuscation Hardness
- Further Research

Summary

What can we do here?

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Further Research

What can we do here?

⇒ Just new transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

What can we do here?

- ⇒ Just new transformations
- Preventive transformations

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What can we do here?

- ⇒ Just new transformations
- → Preventive transformations
- ⇒ Protection against recompilation

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What can we do here?

- ⇒ Just new transformations
- → Preventive transformations
- ⇒ Protection against recompilation
- ⇒ Introducing more deobufuscation hardness results

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What can we do here?

- ⇒ Just new transformations
- → Preventive transformations
- ⇒ Protection against recompilation
- ⇒ Introducing more deobufuscation hardness results

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

What can we do here?

- ⇒ Just new transformations
- → Preventive transformations
- ⇒ Protection against recompilation
- Introducing more deobufuscation hardness results

Good Luck with this stuff!

Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

Obfuscator analyse and modify program by series of transformations



Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness

Further Research

Summary

- Obfuscator analyse and modify program by series of transformations
- Obfuscating transformations consist of layout, data and control tricks



Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

- Obfuscator analyse and modify program by series of transformations
- Obfuscating transformations consist of layout, data and control tricks
- ⇒ Hardness of deobfuscation is not proved



Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

- Obfuscator analyse and modify program by series of transformations
- Obfuscating transformations consist of layout, data and control tricks
- ⇒ Hardness of deobfuscation is not proved



Yury Lifshits

What is Obfuscator?

Notion of Obfuscator Anatomy of Obfuscator Obfuscator Characteristics

Obfuscation Library

Program Representation

Data & Control : Basic Tricks

Control Flow Obfuscation

Even more transformations

Obfuscation vs. Deobfuscation

Classical Program Analysis Deobfuscation Hardness Further Research

Summary

Obfuscator analyse and modify program by series of transformations

Summary

- Obfuscating transformations consist of layout, data and control tricks
- ⇒ Hardness of deobfuscation is not proved

Question Time!
Obfuscating Transformations

Not covered by the talk

Yury Lifshits

Back Up Slides

Not covered by the talk

Obfuscation vs. watermarking

Obfuscation for watermarking

Making disassembling hard.

Decompiled – uncompilable for Java

General idea – make program dictionary as short as possible

Preventive obfuscation

Profiling in the obfuscator

Reducible and non-reducible graphs

Are obfuscating transformations comparable, e.g. one OT is every time better than another OT?

Program Analysis classification

Obfuscating Transformations

For Further Reading

Yury Lifshits

Back Up Slides

Not covered by the talk References



Collberg - Thomborson - Low Series of papers

http://www.cs.arizona.edu/~collberg/research/publications/