All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution
(but might have been afraid to ask)

Matteo Di Pirro

BSc in Computer Science
Department of Mathematics

University of Padova

December 7, 2016

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Outline

Introduction

Static and Dynamic Analysis

- **Static Analysis**
  - Examines a program's text to derive properties that hold for all executions
  - Program-centric analysis
- **Dynamic Analysis**
  - Examines the running program to derive properties hold for one or more executions
  - Detect violations of stated properties
  - Provide useful information about the behavior of the program
  - Input-centric analysis

Dynamic Analysis

There are two essential questions about the input analysis:

Dynamic Analysis

There are two essential questions about the input analysis:

1. **Is the final value affected by user input?**
    - **Dynamic Taint Analysis**!
    - Tracks information flow between sources and sinks

Dynamic Analysis

There are two essential questions about the input analysis:

1. **Is the final value affected by user input?**
   - **Dynamic Taint Analysis**!
   - Tracks information flow between sources and sinks
2. **What input will make execution reach this line of code?**
   - **Forward Symbolic Execution**
   - Allows us to reason about the behavior of a program on many different inputs

Università
degli Studi
di Padova

Thank you for allowing me to taint your precious time!

Dipartimento
Matematica