UNIVERSITÀ DEGLI STUDI DI PADOVA

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

DIPARTIMENTO MATEMATICA

Outline

UNIVERSITÀ DEGLI STUDI DI PADOVA

Introduction

Dynamic analisys

UNIVERSITÀ DEGLI STUDI DI PADOVA

There are two essential types of dynamic analisys:

Dynamic analisys

There are two essential types of dynamic analisys:

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

Dynamic analisys

There are two essential types of dynamic analisys:

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

Università
degli Studi
di Padova

Thank you for allowing me to taint your precious time!

DIPARTIMENTO
MATEMATICA