FACULTATEA DE
AUTOMATICĂ ȘI
CALCULATOARE
Universitatea POLITEHNICA din București

Dynamic Taint Analysis

Ioana BRĂNESCU
Andreea-Larisa COZUC
Andreea-Diana OLTEAN
George-Andrei IOSIF

Introduction

- Manual security assessments are no longer viable
- As an alternative, automated vulnerability detection
  - Fuzzing
  - Symbolic execution
  - Taint analysis
    - Static
    - Dynamic, both online and offline

TaintCheck

- Functionalities
  - Detection of overwrite attacks
  - Exploit analysis for signature generation
  - Significant overhead
- The process consists of four steps:
  - Marking inputs as tainted based on the policy
  - Instrumentation for tracking the taint propagation
  - Detection of sensitive memory overwrite
  - Automatic semantic analysis on exploit, for signature generation

SwordDTA

- Functionalities
  - Detects four types of vulnerabilities
    - Buffer overflow
    - Integer overflow
    - Division by zero
    - Use-after-free
  - Implemented via Pin DBI
- The process consists of three steps:
  - Taint introduction
  - Taint propagation
  - Vulnerability detection

OFFTAN

- Functionalities
  - Uses an offline approach
  - Detects two types of vulnerabilities:
    - Stack buffer overflow
    - Controlled jumps
- The process consists of four steps:
  - Dynamic information acquisition
  - Vulnerability modelling
  - Offline analysis
  - Backtrace analysis

Strengths

- Binary translation into Assembly or UCode
- Null false positive rate
- Exemplification through case studies
- Distributed techniques

Weaknesses

- Lack of proactive exploit detection
- Evasion of the proposed solutions
- Small test cases
- None or only relative evaluations

Related Efforts

- Fuzzing and artificial intelligence integration
- Ongoing research on:
  - Different programming languages: JavaScript
  - Different platforms: Android
- Whole-system approach

Conclusions

- Really useful, when attempting to discover vulnerabilities
  - Online, during runtime
  - Offline, by using trace files
- Significant overhead
- Continuous progress