Smash File Fuzzer

Presented at OWASP AppSec Research 2010

By Komal Randive, Symantec Corporation

23 June 2010

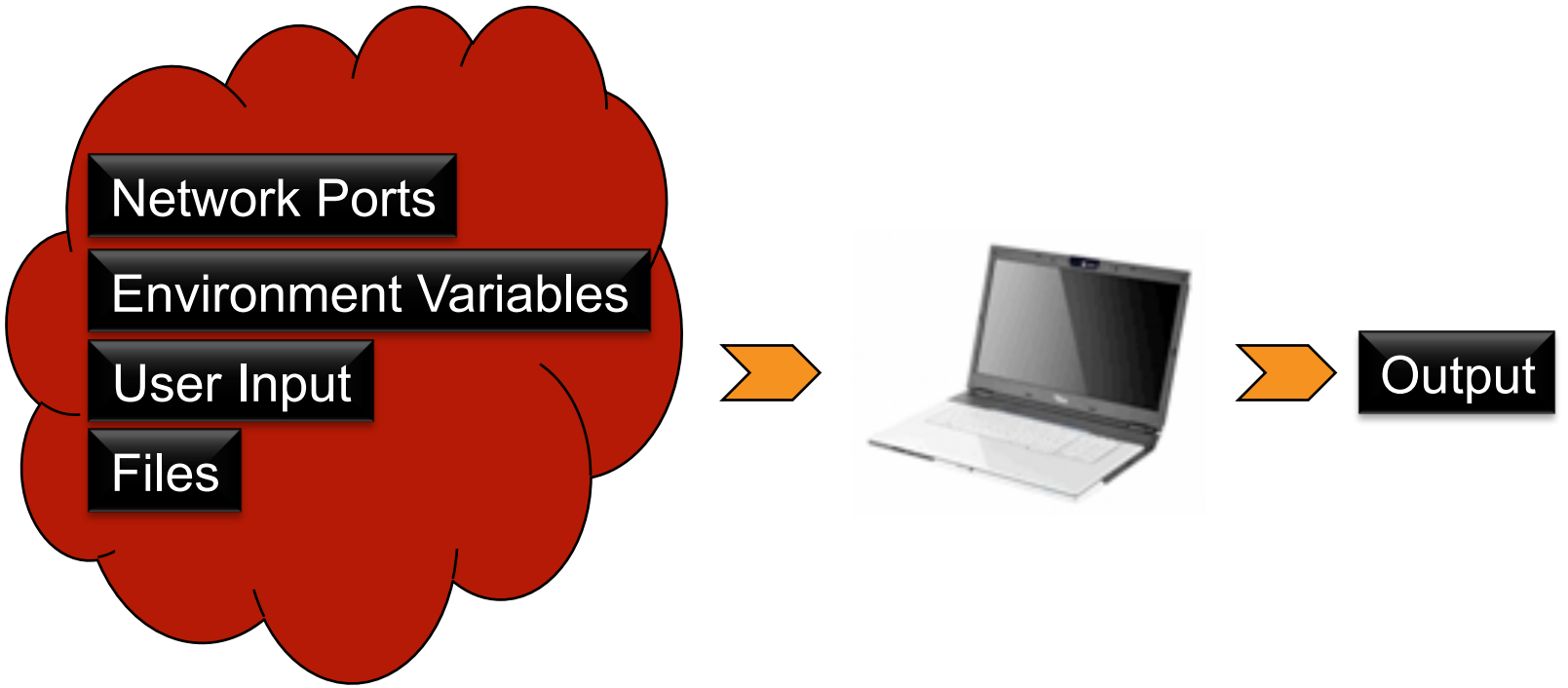
Introduction

- Symantec Product Security Group
- Safe Code www.safecode.org

Agenda

1. Why File Fuzzing ?
2. Smash File Fuzzer
3. File Categories
4. Fuzzing with greater control
5. Demo
6. Future of Smash File Fuzzer

Why File Fuzzing?

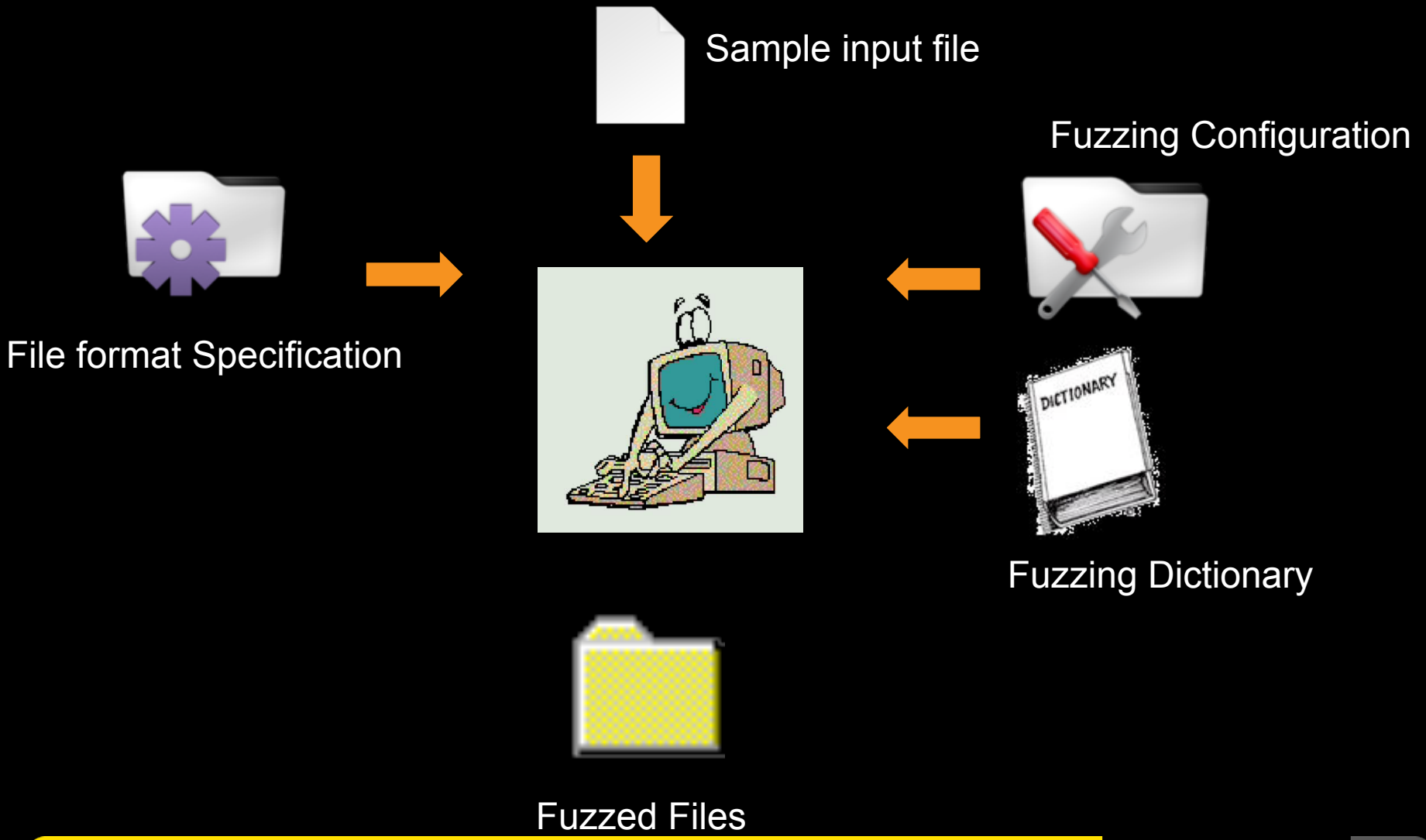


Why File Fuzzing?

Yet Another File Fuzzer ?

- Controlled fuzzing – guarantee file acceptance by application
- Partial file format specification
- Fuzzing Compound files
- Coverage and compliance

Smash File Fuzzer



Inputs for Smash File Fuzzer

- File format specification
  - Custom Description language
  - Field length, offset, field hierarchy, field sequence
- Fuzzing Configuration
  - What to fuzz ?
  - How to fuzz?

  <field name> <occurrences to be fuzzed> <attack type> <length update>
- Fuzzing Dictionary
  - Attack specific fuzz input strings
  - Application specific data

File Categories

- Standard file formats
  - Format specifications are precise
  - Contains magic strings
  - Hierarchy of subfields
  - ASCII and binary data
    - E.g. .rtf , .wav , .png etc.
- Application specific configuration files
  - Custom defined and weak format specifications
  - Delimiters as magic strings
  - Relatively flat subfield hierarchy
  - Mostly ASCII data
    - E.g. .cnf , .xml, .conf , .csv etc
- Data files
  - Format specification is very precise
  - Contains no magic strings
  - Binary data
    - E.g. .dat

Fuzzing with greater control

- File fuzzing with partial file format description
- Targeted attack specific fuzzing
  - Buffer overflow, format string attack, directory traversal, SQL injection etc.
- Higher control over the fuzzing
  - Fields to be fuzzed
  - Occurrences to be fuzzed
  - Application specific data
  - Multiple field fuzzing
  - Number of fuzzed files to be generated
  - Length update option

Demo

CVE-2008-2430 - Integer overflow in VLC Media Player via a large fmt-chunksize value in a WAV file.

Future of Smash File Fuzzer

- Build a library of file format specifications
- Detailed correlation among fields in file format

Thank you!

Komal Randive

Komal_randive@symantec.com