What the fuzz?

Fuzzing and debugging

Renne Jämsén

Contents

- What is fuzzing?
- Why to fuzz?
- How to fuzz?
- Demo

What is fuzzing?

A technique to find out bugs and security flaws in computer systems using automated inputs.

What is fuzzing?

- First used in 1988 at University of Wisconsin by Prof. Barton Miller
- Started as a class project
- Project goal: a program that tests the robustness of UNIX utilities i.e. a fuzz generator

Miller, B. 1988

From: Barton Miller

Sent: Wednesday, February 16, 2005 4:39 AM

To: Shawn Hernan

Subject: Re: origins of the term "fuzz"

Thanks for the note. As far as I know, I coined the term.

The original work was inspired by being logged on to a modem during a storm with lots of line noise. And the line noise was generating junk characters that seemingly was causing programs to crash. The noise suggested the term "fuzz".

--bart miller

Correspondance between Miller, B. and Hernan, S. (Neystadt, J. 2009)

Different kinds of fuzzing

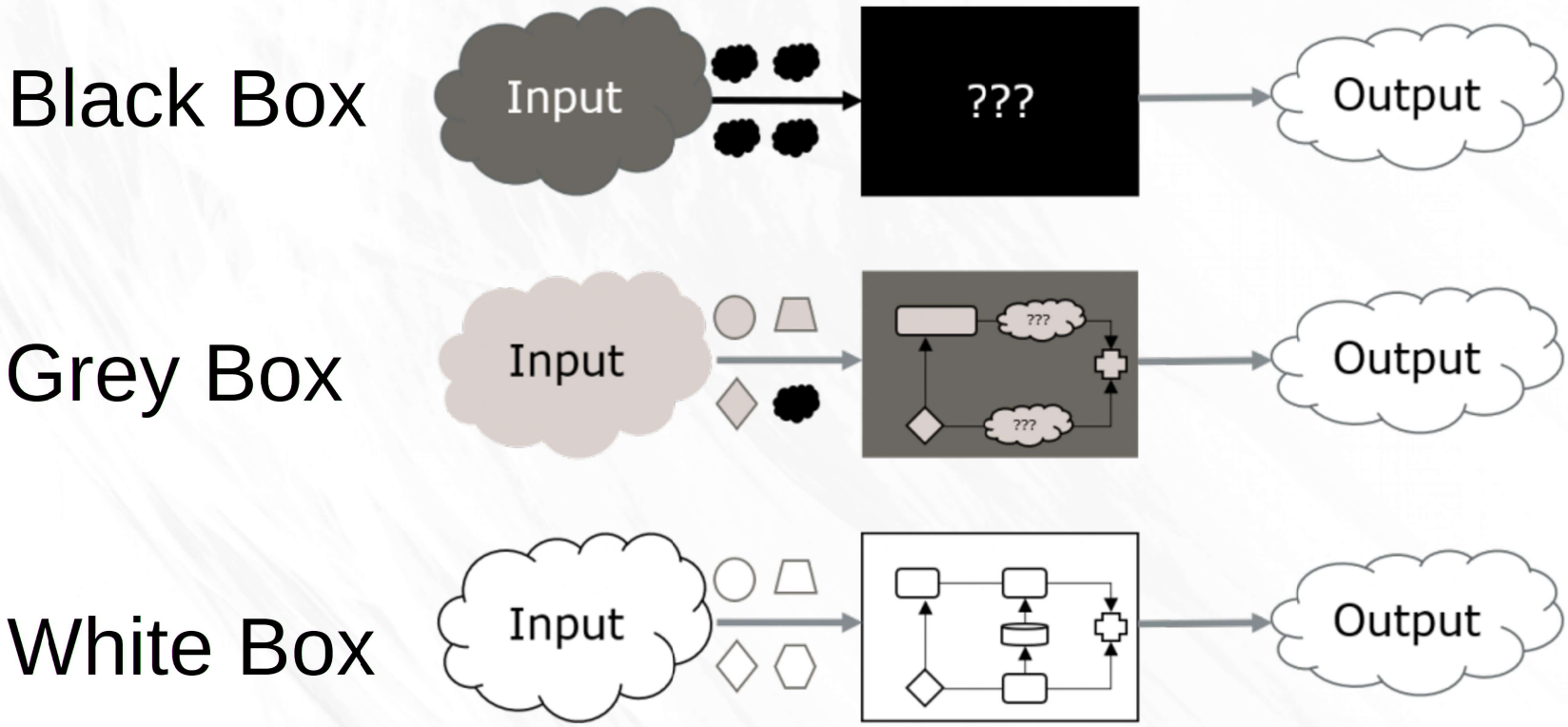

Image source: https://www.coderskitchen.com/fuzzing-techniques/

Why to fuzz?

- To map attack vectors that could be exploited to gain access into your system
- To discover program breaking cases of user input (malicious and unmalicious)
- Recommended by international standards in many fields

International standards that require or recommend fuzzing

ISO 26262
Road vehicles – Functional Safety

UNECE WP.29
United Nations World Forum for Harmonization of Vehicle Regulations

ISA/IEC 62443-4-1
Secure Product Development Lifecycle Requirements

ISO/SAE DIS 21434
Road Vehicles — Cybersecurity Engineering

UL2900-1 and **UL2900-2-1**
Healthcare and Wellness Systems - Software Cybersecurity for Network-Connectable Products

ISO/IEC/IEEE 29119
Software and Systems Engineering - Software Testing

ISO/IEC 12207
Systems and Software Engineering – Software Life Cycle Processes

ISO 27001
Information Technology – Security Techniques – Information Security Management Systems

ISO 22301
Security and Resilience — Business Continuity Management Systems

IT-Grundschutz (Germany)
Based on ISO 27001

NIST SP 800-95
Web Services — standard for software testing (USA) and others

Image source: https://www.code-intelligence.com/what-is-fuzz-testing

How to fuzz?

- Use a fuzzer
- ffuf (MIT License)
  - fuzzes a wordlist against a target (Hoikkala, J. 2021)
- Radamsa (MIT License)
  - Test case generator, mutates inputs (Helin, A. 2013)

Other fuzzing tools

- beStorm by Beyond Security
- CI Fuzz by Code Intelligence
- Fuzzing Test Suite by Synopsys (toolkit)
- Mayhem by ForAllSecure

(Breeden, J. 2022)

When to fuzz?

- Preferably all the time
- More mutations tested = more robust system

Sources:

Helin, A. 2013. A Crash Course to Radamsa. https://gitlab.com/akihe/radamsa/-/blob/develop/README.md?ref_type=heads. Accessed: 2023/10/07

Hoikkala, J. 2021. ffuf documentation. https://github.com/ffuf/ffuf/wiki. Accessed: 2023/10/07

Miller, B. 1988. Project List. Computer Sciences Department University of Wisconsin-Madison. https://pages.cs.wisc.edu/~bart/fuzz/CS736-Projects-f1988.pdf. Accessed: 2023/10/06

Neystadt, J. 2009. Automated Penetration Testing with White-Box Fuzzing. Microsoft Corporation. https://learn.microsoft.com/en-us/previous-versions/software-testing/cc162782(v=msdn.10). Accessed: 2023/10/02