|  |
| --- |
| User’s Guide (Pit File Mode) |
| 2013-2014 |
| By Rakotyansky Maria |

Contents

[1. Introduction 3](#_Toc398731048)

[2. Installation 3](#_Toc398731049)

[3. User Instructions 3](#_Toc398731050)

[3.1. Mode Choice 3](#_Toc398731051)

[3.2. Pit File Mode 3](#_Toc398731052)

[3.3. Select GA Strategy 5](#_Toc398731053)

[3.4. Start Session 6](#_Toc398731054)

[3.5. Statistics 6](#_Toc398731055)

# Introduction

The Evolutionary Fuzzing Framework allows analyzing the target software vulnerabilities with the help of the predefined list of Genetic Algorithms.

Genetic Algorithm to be used is built of several elements:

* Parents Selection Strategy
* Survival Strategy
* Percent Of Mutation
* Number Of Elements In Population

The GUI allows selecting different combinations of elements what makes the system flexible.

In addition to this the user can insert other parameters which will be described below to simplify the data collection and its storage.

# Installation

All project’s program files are contained in the folder “Evolutionary Fuzzing Framework Source”.

Before running the program, please, make sure that Peach Fuzzer is installed. The version used: Peach 2.3.9 (python).

Please take into the consideration the fact that it was slightly modified. The ability to return the average test case time through the log file status.txt was added. The modified version can be found in the directory **PeachFuzzerVersion**. See file **peach\_svn\_2.3.9.rar.** Full installation instruction can be found at <http://old.peachfuzzer.com/v2/PeachInstallation.html>.

# User Instructions

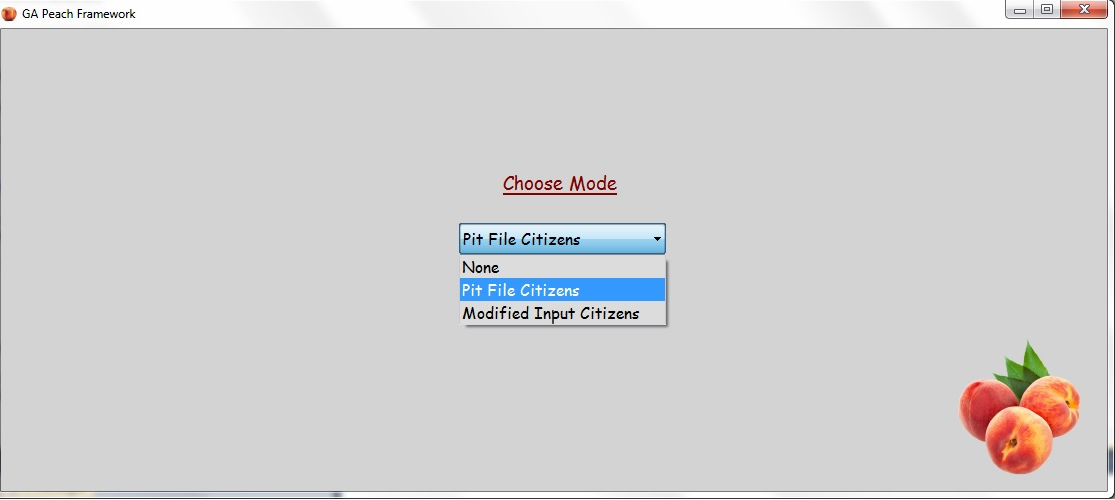
# Mode Choice

Upon running the Evolutionary Fuzzing Framework, GUI is displayed. First of all it allows choosing the mode of The Evolutionary Fuzzing System work. See **Figure 1.**

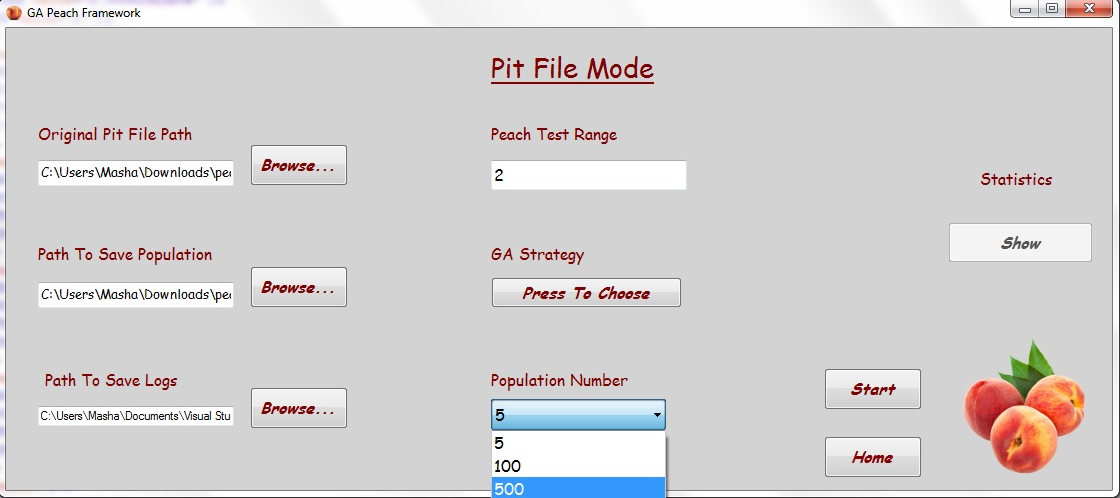
# Pit File Mode

After the “Pit File Citizens” mode is chosen the User sees the Pit File Mode window. See **Figure 2.**

Here the user should choose the Original Pit File Path, i.e. the path to the Peach Pit file which will be used as a source for creation of the initial population. Each element of the initial

**Figure 1**: Choose Mode Window

**Figure 2**: Pit File Mode

****

population is a modified (mutated) version of the original Peach Pit file. Mutations are done randomly.

Then the User should choose the Path To Save Population. That is to give the program instruction where to keep elements of the current generation.

Also can be chosen Path To Save Logs, i.e. a directory for keeping the logs returned by the Peach Fuzzer Platform. This might be important for further analysis of the session results.

Population Number drop-down box gives 4 options: 5, 100, 500 and 1000 elements.

Peach Test Range determines number of test that Peach Fuzzer will run on every citizen.

To choose the Genetic Algorithm configuration for the current session the user must press the button “Press To Choose”.

It will pass to the next window which you can see in **Figure 3.**

**Figure3:** Select GA Strategy

****

# Select GA Strategy

Fitness Strategy includes 3 options:

* **Good Files Only:**

for breeding should be used only valid Peach Pit files, i.e. only Peach Pit files that can be accepted and processed by the Peach Fuzzer platform.

* **All Bad Files:**

for breeding can be used all the population elements, no matter whether they are valid or not. Just pay attention please that in case the Peach Pit file is invalid its fitness value is equal to 0.

* **Bad Files Partially:**

for breeding can be used all valid files and a certain predefined percent of invalid files. When this option is chosen the window “% Of Children with Bad Files” will be activated.

“Parent Choice Strategy” drop-down box includes 3 options: Naïve (random choice of parents), FPS, and Tournament. The algorithms details can be found in the file FuzzingProject.docx.

FPS option includes extra variation: with scaling and without scaling. “WithScaling” checkbox is activated after choice of “FPS” option.

Mutation Rate determines the mutation probability of a newborn child. The possible range is from 0 to 1.

Number of iterations is in fact a number of generations to be created consequently during the current session.

Another important parameter is Survival Strategy. The following options are offered: Elitism, Aging, and Genitor. The strategies details can be found in the file FuzzingProject.docx.

In accordance to the chosen option will be activated text boxes ElitRate, GenitorRate, MaxAge.

Please pay attention that values of ElitRate and GenitorRate are given in percent.

After all the parameters are chosen buttons “Apply” and “Return” should be pressed. The user will return to the window “Pit File Mode”. See **Figure 2**.

# Start Session

If all the parameters are selected and are valid the user should press button “Start” in the window “Pit File Mode”.

# Statistics

After the run of the program is ended, the button “Show” in the “Pit File Mode” window is activated. After pressing it the user passes to the “Statistics” window. In the left side of the window all the parameters of the current session are returned.

To see the chart a necessary parameter should be chosen in the drop-down box in the upper right corner of the window.

The options are:

* **Invalid Pits (%) Per Iteration:**

Percent of Peach Pit files that cannot be accepted and processed by the Peach Fuzzer platform. As a result their fitness value is 0.

* **Convergence Per Iteration:**

Shows number of groups including identical Peach pit files in the population of a given size per iteration

* **Average Fitness Per Iteration:**

Shows average fitness in the population of a given size per iteration.

* **% Of Fault Pits:**

Shows percent of Peach Pit files that provoked fault or crash of the target software.

* **All:**

Show all data mentioned above.

To save the data outputted in the window user should press button “Save”. Here he will be able to choose a path to save directory with data.

To add other charts the user should press button “Update”.

The directory with fault outputs is kept in the directory “Faults” in accordance with path chosen to save population.