Detection Algorithm for Non-recursive Zip Bombs

Authors:
MaoYang Chen
University of Electronic Science and Technology of China
MingYu Fan
University of Electronic Science and Technology of China
Presenter:
MaoYang Chen
maplejack@qq.com

MaoYang Chen

- UESTC Bachelor Degree
- Master student in UESTC
- Used to be an international volunteer in Sri Lanka

Abstract

The traditional zip bombs rely on a recursive structure, but recently a type of zip bombs with non-recursive structure has appeared. We conducted research on this and gave a detection method.

The differences of info-zips and the bombs

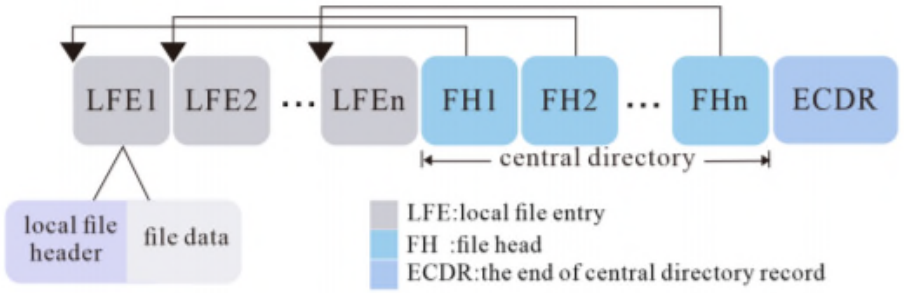

Figure 1: The structure of info-zip

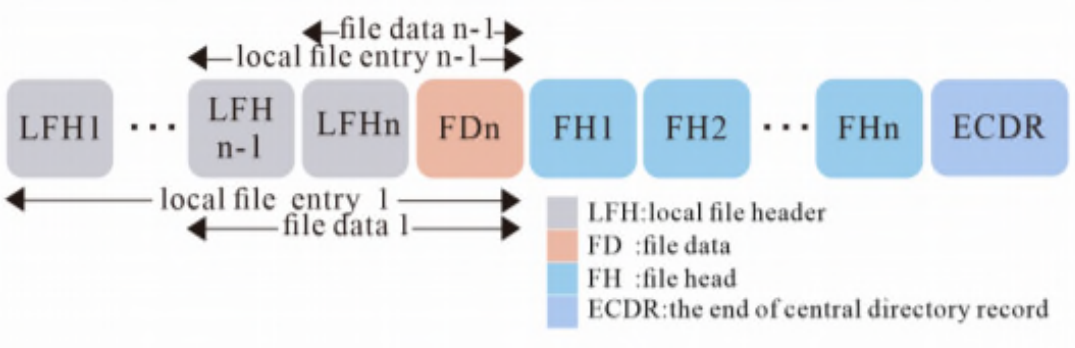

Figure 2: The structure 1 of the non-recursive zip bombs

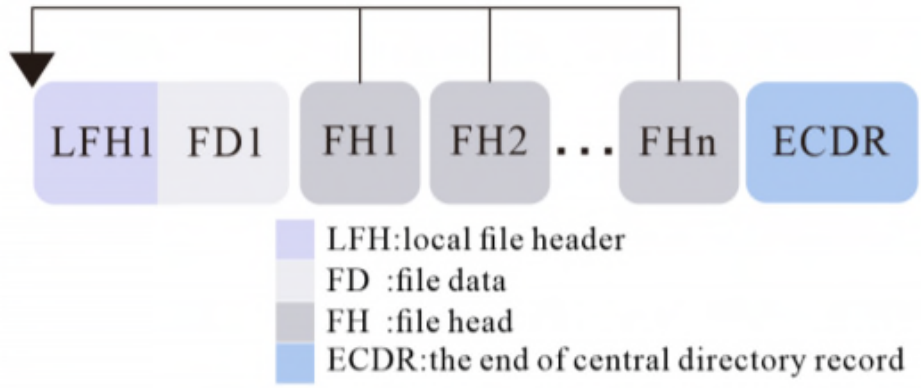

Figure 3: The structure 2 of the non-recursive zip bombs

The basic idea of detection

Non-recursive zip bombs depend on its overlapping structure, so the most important and basic idea for detecting such bombs is to detect whether the target zip file contains such overlapping structures.

Detection steps

- Open the target zip file in hexadecimal
- Find the positions of each local file entry
- Check whether these local file entries overlap

Some questions that need attention

- The problem of small-endian and big-endian
- Fake file headers
- The search method

Efficiency

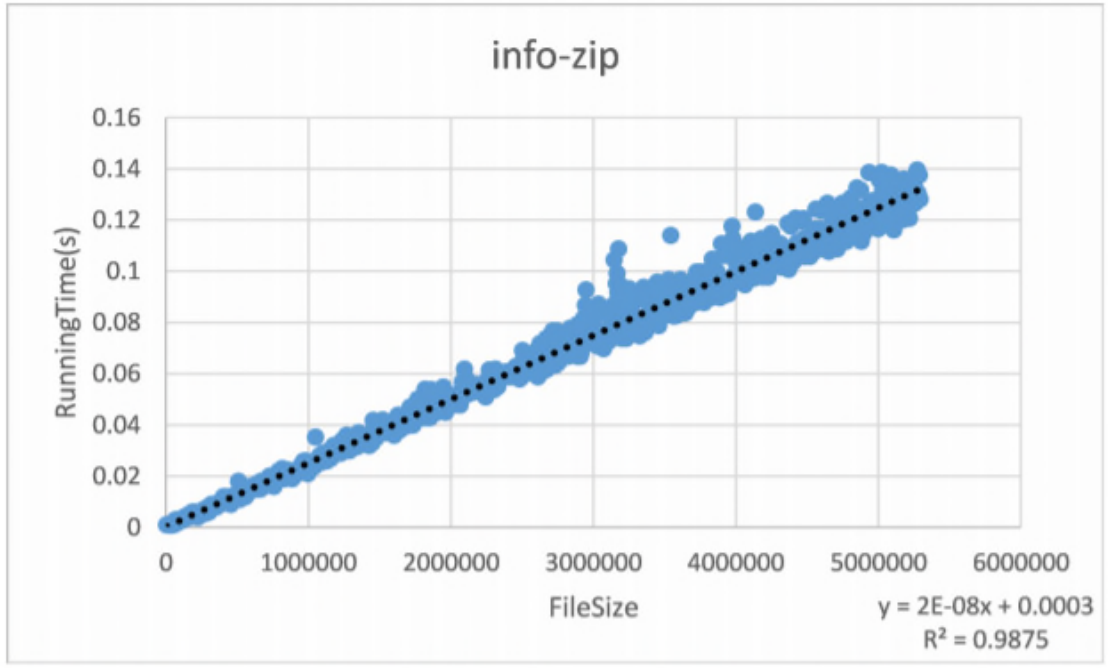

Figure 5: The relationship between the detection time and the size of info-zip

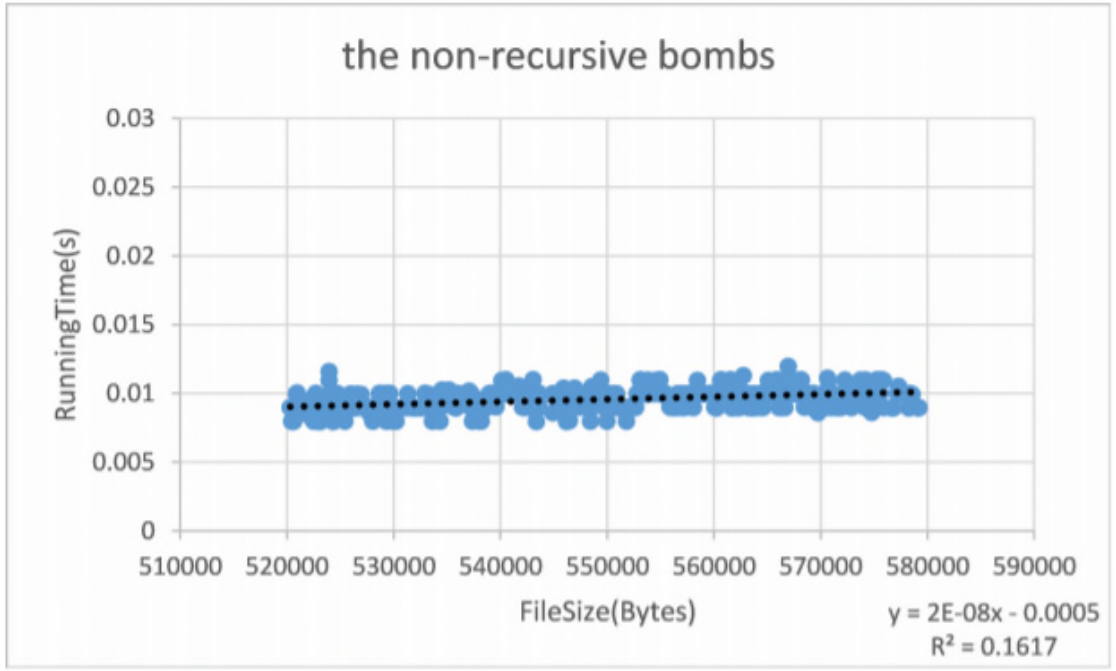

Figure 6: The relationship between the detection time and the size of the non-recursive zip bombs

Thank you