ДЕМОНСТРАЦИЯ EXE ОБФУСКАТОРА

Научный руководитель
к. ю. н., доцент
Горев А. И.

Выполнил студент группы
СИБ-941-ЗИ-01
Москалев К. Н.

ЧТО ТАКОЕ ОБФУСКАЦИЯ?

Обфуска́ция (от лат. obfuscare — затенять, затемнять; и англ. obfuscate — делать неочевидным, запутанным, сбивать с толку) или запутывание кода — приведение исходного кода или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

ПОЧЕМУ ИМЕННО EXE И PYTHON?

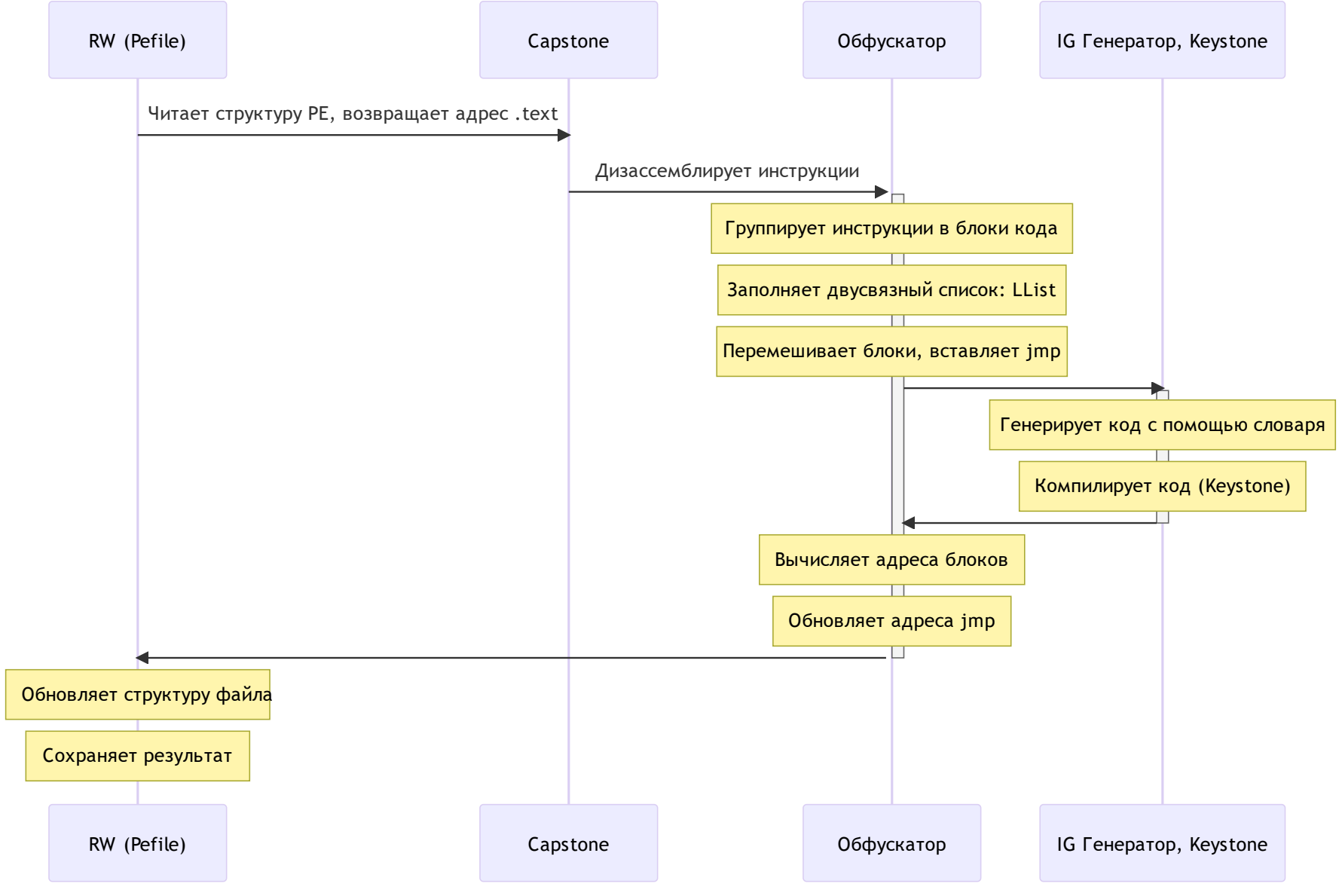
Преимущества 💪:

- Больше возможностей для запутывания.
- Поддержка вне зависимости от языка.
- Возможность контроллировать процесс.
- Keystone - одно из лучших решений реверса.
- Легкий и наглядный концепт, который легко развить до реального решения.

Недостатки ❌:

- Python не самое быстрый язык программирования из коробки.
- Нужно точно вычислять адресс прыжков.
- Нужно уметь читать разные варианты PE структуры.
- Требует базового понимания реверсинга.

СТРУКТУРА

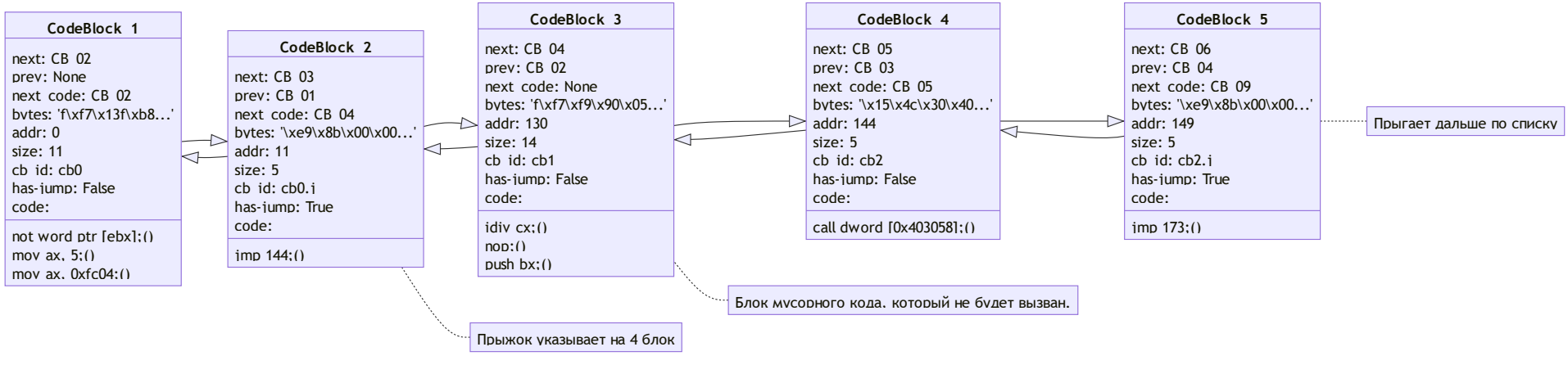

RW (Pefile)
Capstone
Обфускатор
IG Генератор, Keystone
Читает структуру PE, возвращает адрес .text
Дизассемблирует инструкции
Группирует инструкции в блоки кода
Заполняет двусвязный список: LList
Перемешивает блоки, вставляет jmp
Генерирует код с помощью словаря
Компилирует код (Keystone)
Вычисляет адреса блоков
Обновляет адреса jmp
Обновляет структуру файла
Сохраняет результат
RW (Pefile)
Capstone
Обфускатор
IG Генератор, Keystone

ГЕНЕРАЦИЯ КОДА

```
# mnemData.py ...
[10, # Add two values.
  mnem('add', rm_rmi)],
[1, # Add with carry.
  mnem('adc', rm_rmi)],
[2, # Logical and.
  mnem('and', rm_rmi)],
[1, # Bit scan forward. 1 op get number, 2 op scan for bits. If 0 only, then ZF =
  mnem('bsf', r_rm, (2, 3))],
[1, # Bit scan reverse.
  mnem('bsr', r_rm, (2, 3))],
[1, # Bit test. 1 op from take the bit, 2 op number of bit. CF have the value of b
  mnem('bt', rm_rl, (2, 3))],   # "mw 1" for 4
```

```
# instGenerator.py ...
def make_inst(self) -> Inst | None:
  """Создает инструкцию"""
  mnem_data = choose_inst(self.insts, self.probs)
  ops = self.make_args(mnem_data['ops'], mnem_data['size'], mnem_data['ops_size'])
  instruction = Inst(mnem_data['mnem'], ops)
  try:
    instruction_updated = self.c.asmu(instruction)
  except KsError as ex:
    lg.error('KsError:%s'%(ex), exc_info=True)
    return None
  return instruction_updated
```

ДВОЙНОЙ СВЯЗНЫЙ СПИСОК



ИСПОЛЬЗОВАННЫЕ ИНСТРУМЕНТЫ

- Pefile - Парсер и редактор PE структуры исполняемого файла.
- Keystone\Capstone - Компилятор и дизассемблер с API.
- FASM - удобный и поддерживающийся язык ассемблера и компилятор.
- x64dbg - Современный дебаггер
- 010 Editor\ Hex Neo - Hex редакторы
- IDA pro - мощный инструмент для реверсинга
- VS code - IDE

ВРЕМЯ ДЛЯ ДЕМО!