Программа Ghidra – реверс-инжиниринг

Задача – восстановить большую часть логики игры

Самое важное – восстановить структуры данных. Структура данных – последовательность байт с типами. На физ. уровне типы сложно различимы – только разве их длина. Правда иногда на это намекает тип регистра(xmm - float), но все равно сложно. В любом случае главное – восстановить структуры, придав их полям осмысленные названия.

struct Player

{

int type,

float[3] pos,

float[16] matrix

}

Как восстановить структуру? Алгоритм:

1. Найти базовый адрес структуры, зная, что это действительно структура, а не массив.
2. Определить конец структуры – достаточно узнать размер. Размер можно получить:
   1. Через аллокатор, который выделил в куче память. Как правило он спрятан в конструкторе класса(этой структуры) или может быть снаружи.
   2. Если это стек – то под структуру резервируется память статически. Здесь сложно определить размер, ибо поля сливаются с локальными переменными на физ. уровне. Решение – сгруппировать поля по смыслу и выделить их в структуру. Можно глядеть в какие функции передается структура и с какими её полями(смещениями) она работает.
   3. Если не удается определить, то размер структуры – макс. смещение, которое для нее найдено.
3. Если определен размер и известен адрес, то для нас это пока что массив байт.

Теперь нужно определить поля структуры, пока что без типов. Важно получить список функций, которые работают с данной структурой. Если найдено что-то типа такого: [rcx+0x14], то сразу ясно начало поля структуры. Очевидно, что с 0x10 по 0x18 нет типа размера 8(например указателя) и что тут вполне может быть тип: int, float, bool

Однако обращение к полям происходит с указанием размера: byte, word, dword, qword. Поэтому легко определить и конец поля. Например: dword[rcx+0x14] – получение int или float значения(ну или bool). Необходимо обращать внимание на выравнивание. Очевидно, что указатель после этого поля(с адреса 0x14) начинаться не может.

1. Определив всевозможные поля, можно далее подразделить поля на int и float по регистрам. Также легко определить указатели. Сложнее различить int, byte и bool: нужно смотреть на значения.

Восстановленная структура – это определение всех полей и их типов, а также множество методов(функций), работающих с данными полями. Так как все современные приложения – это ООП, то все строится на структурах. Ибо структура описывает некоторый объект: игрока, машину, задачу, камеру, элемент интерфейса.

Содержание структур в играх – это состояние игры в данный момент времени. То, что мы видим на экране – это определенные значения в структурах. Поэтому методы могут просто изменять некоторые поля, при этом будет казаться в игре, что они меняют картинку, физику и т.д. В силу этого, можно сделать копию структуры и применять к ней методы, следя, какие поля она изменила и на что изменила при текущем наборе аргументов. Меняться глобальное состояние не должно в силу инкапсуляции.

Пример: у нас есть сущность, у которой есть кости(bones). Сделать возможность просмотра координат этих костей, визуализацию через directx, изменение положения и… сделать программирование через луа работу с этими значениями, возможно перезапись и тд

Стек, локальные переменные

|  |
| --- |
| 0x28: 5-й аргумент |
| 0x20: регистр |
| 0x18: регистр |
| 0x10: регистр |
| 0x08: регистр |
| 0x00: **адрес возврата (rax, rbp)** |
| -0x08: регистр |
| -0x10: … |
| -0x18: локальные переменные |
| -0x20: … |
| -0x28: регистр |
| -0x30: регистр |
| -0x38: регистр |
| -0x40: **адрес возврата** |
| -0x48: … |

Функция 1: sub rsp, 0x38 (место выделяется не только для лок. Переменных, но и для сохранения регистров в функциях, которые вызываются в данной функции + для 5-ого, … аргументов)

Адрес возврата хранится с 0x00 по 0x08.

Часто обращение к локальным переменным происходит через регистр rsp(а не rbp). Смещение относительно адреса возврата можно расчитать так: rbp = rsp + offset (rbp – указывает на адрес возврата, offset – значение в текущем месте), откуда rsp = rbp – offset. Заменяем это в текущей формуле:

[rsp + 0x18] -> [rbp + 0x18 - offset]

offset считается как сумма смещений, производимых функциями sub rsp, push, pop, …

Путь до выявления определенной функции

1) Синтез

2) Анализ

3) Концевая ф-я

Это 2 самых простых случая. Рассмотрим более сложные случаи - их комбинации.

1) Синтез & Анализ

Далее рассмотрим небольшой граф.

gvar

Задача: алгоритмически найти самый простой путь, чтобы разузнать, что данная функция делает. Простота складывается из минимального времени, нужного для реверсинга каждой вершины на этом пути. Дополнительные параметры – избегание вершин-методов некоторого класса или функций, у которых есть/нет определенные теги. Выбирать на пути преимущественно маленькие функции, желательно без виртуальных вызовов. Также учитывать глобальные переменные и прокладывать путь через мосты (синие линии).

На каждой вершине пути можно автоматически юзеру предлагать делать одну из вещей: debug, …

Хранить список пройденных вершин для ускорения.

Необходимо найти лучший из всех путей -> на каждом шаге пробовать все развилки и в итоге выбрать лучшую. Так как алгоритм поиска рекурсивный, то все действия одинаковы для всех вершин. Есть стартовая вершина(красная) и параметры поиска – это вход для алгоритма.

Алгоритм прост: сначала для стартовой вершины сравниваем структуру с одним из 3 базовых шаблонов. Если не совпало с каким-то, пытаемся рекурсивно вызвать данный алгоритм для тех вершин, из-за которых не совпало и т.д.

Находить можно все возможные пути, однако сортировать их в порядке простоты.

Концевые функции и задача синтеза

По сути, эти 2 задачи хоть и являются базовыми, но не являются тривиальными. Концевая функция может:

1. Вызывать API функцию (открыть файл, создать поток, …).

Тут всё просто.

1. Каким-то образом модифицировать входящие аргументы или возвращать какой-нибудь результат (работа со строкой, мат. функция, …).

Нужно просто дебажить или догадываться.

1. Изменять некоторую структуру, т.е. являться методом класса.

Если это метод неизвестного класса, и он изменяет неизвестные нам поля, то:

1. Изменять или читать неизвестную глобальную переменную.

Тогда идем по мосту глобальной переменной в те области программы, где легко выявить, что она обозначает.

Выбор функции автоматически, которую можно отреверсить

Где можно еще применить вышеописанный алгоритм, дак это для поиска следующей функции в программе, которую легко распознать.

Для этого проходимся циклом по всем функциям в программе, для каждой вызывая поиск пути. Заносим их в пул пройденных вершин, где для каждой пройденной функции легко вычислить сложность реверсинга, так как для каждой вершины вызывается поиск пути. Сначала можно вычислить сложности, отсортировать функции, а потом для каждой функции по отдельности вызывать поиск пути уже для пути. Можно также умножать на спец. коэффициент, который нужен для вывода в топ только тех функцией, чей реверсинг поможет на потом (число ссылок, глубина)

Создание структур

1. Найти аллокатор и деаллокатор памяти. Их может быть несколько.
2. Хукнуть их все, при каждом вызове заносить в таблицу адрес, время в нс, кол-во выделенной памяти и адрес возврата (map).

Легко найти: время жизни объекта, конструктор (адрес возврата), деструктор, размер структуры

1. Хукнуть все функции, куда может передаваться аргументом объект или возвращаться. При каждом вызове такой функции проверять наличие объекта в таблице. Для каждого объекта заносить функцию, которая для него вызывается (список ид функций), причем важен порядок. Первая вызванная функция – конструктор, последняя – вероятно деструктор. Также делать ***снимки*** объектов и заносить в буфер, а потом в файл!

Пример:

|  |  |  |  |
| --- | --- | --- | --- |
| Адрес в куче | Размер | **Адрес возврата** | Список функций |
| 0x1000 | 0x10 | 0x40000 | 102, 44, 105 |
| 0x2000 | 0x320 | 0x40010 | 45, 21 |

Адрес возврата – ключевое поле. По нему мы определяем уникальность объекта.

1. Как только вызывался конструктор, у которого тот же адрес в куче, то перенести инфу об объекте в другой массив.
2. После того, как таблица в течение долгого времени не возрастает в плане новых объектов, то мы можем получить что-то типа следующего:

|  |  |
| --- | --- |
| Размер | Список функций |
| 0x30 | **25**, 33, 100, 103, 670 |
| 0x34 | **25**, **100**, 103, 107 |
| 0x40 | **25**, **100**, 105 |
| 0x100 | 56, 89 |

Каждая строка – какой-то объект.

Мы видим, что у первых 3-х строк есть функция 25. Более, того – она вызвалась первой во всех случаях. Значит это конструктор для какого-то базового класса. 100 – так же конструктор базового класса. Базовый класс может быть абстрактным и не иметь конструктора. Тогда здесь не всё так просто, см. далее.

1. Давайте построим иерархию

0x30

0x34

0x40

0x100

107

33, 100, 103, 670

105

Надо также выяснить иерархию конструкторов. Для этого надо проверить, вызывается функция ид 25 из функции ид 33. Если да, то 33 конструктор. Эвристически можно определить, что 25 тоже конструктор, ибо за ним наверняка вызывалась функция аллокатора.

1. После того, как мы определили все классы в программе, надо присвоить им всем функциям. Даже если не все методы вызвались, они легко могут определиться из уже найденных в контексте. Имена функций переименовать в методы тоже или как-то иначе пометить. Можно вызвать специальный мастер, которым легко можно выбрать нужные функции, у которых надо изменить сигнатуру.
2. Далее надо определить оффсеты полей. Для этого придется пройтись по всем найденным методам. Нужно искать чтение и запись в оффсеты структур. Объект может быть получен через аргумент или через другую функцию. Так как мы знаем тип объекта(класс), то можем легко определить поля.

**1 пример**

7ff7896ac61e PUSH RDI

7ff7896ac61f SUB RSP,0x60

7ff7896ac623 MOV **RBX**,qword ptr [**RDX** + 0x10]

7ff7896ac627 MOV RSI,RCX

7ff7896ac62a CMP dword ptr [**RBX** + 0x40],0x0

7ff7896ac62e MOV R9D,dword ptr [**RBX** + 0x48]

7ff7896ac632 MOV R11D,dword ptr [**RBX** + 0x30]

7ff7896ac636 MOVSS XMM0,dword ptr [**RBX** + 0x38]

7ff7896ac63b MOVSS XMM1,dword ptr [**RBX** + 0x20]

7ff7896ac640 MOVSS XMM3,dword ptr [**RBX** + 0x18]

7ff7896ac645 MOV EDI,dword ptr [**RBX** + 0x28]

7ff7896ac648 MOV R8,qword ptr [**RBX** + 0x10]

7ff7896ac64c MOV RDX,qword ptr [**RBX** + 0x8]

7ff7896ac650 MOV ECX,dword ptr [**RBX**]

7ff7896ac652 SETNZ R10B

7ff7896ac656 CMP dword ptr [**RBX** + 0x50],0x0

7ff7896ac65a SETNZ AL

7ff7896ac65d MOV byte ptr [RSP + local\_18],AL

7ff7896ac661 MOV dword ptr [RSP + local\_20],R9D

7ff7896ac666 MOV byte ptr [RSP + local\_28],R10B

7ff7896ac66b MOVSS dword ptr [RSP + local\_30],XMM0

7ff7896ac671 MOV dword ptr [RSP + local\_38],R11D

**2 пример**

7ff789056469 PUSH RDI

7ff78905646a SUB RSP,0x20

7ff78905646e MOV **RDI**,**RCX**

7ff789056471 MOV RCX,qword ptr [**RCX** + 0x370]

7ff789056478 XOR R8D,R8D

7ff78905647b MOV EBX,EDX

7ff78905647d CALL FUN\_7ff789efc6a8

7ff789056482 TEST RAX,RAX

7ff789056485 JNZ LAB\_7ff7890564b0

7ff789056487 MOV RCX,qword ptr [**RDI** + 0x370]

7ff78905648e LEA R8D,[RAX + 0x1]

7ff789056492 MOV EDX,EBX

7ff789056494 CALL FUN\_7ff789efc6a8

**3 пример**

7ff7896bda72 SUB RSP,0x20

7ff7896bda76 CALL GetVehicleById

7ff7896bda7b MOV **RBX**,**RAX**

7ff7896bda7e TEST **RAX**,**RAX**

7ff7896bda81 JZ LAB\_7ff7896bdab7

7ff7896bda83 MOV RCX,qword ptr [**RAX** + 0x20]

7ff7896bda87 MOV ECX,dword ptr [RCX + 0x488]

7ff7896bda8d CALL FUN\_7ff7898d0f20

7ff7896bda92 TEST RAX,RAX

7ff7896bda95 JZ LAB\_7ff7896bdab7

7ff7896bda97 CMP qword ptr [**RBX** + offset DAT\_ffffffffa7da0b90],

7ff7896bda9f JZ LAB\_7ff7896bdab7

7ff7896bdaa1 MOV EDX,0x9

7ff7896bdaa6 MOV RCX,RAX

7ff7896bdaa9 CALL FUN\_7ff7898d0ea0

Алгоритм очень прост. Для этого надо эмулировать работу процессора. У нас есть определенный контекст, в котором находится текущие объекты. Далее мы проходимся по командам и сопоставляем каждому объекту в контексте определенный регистр, в котором он находится. Если есть команда CALL, которая возвращает объект, то заносим объект (его тип) в контекст и сопоставляем его с регистром RAX. Важно: если попалось условие, мы должны разделить проход на два – тут нужно юзать рекурсию. Таким образом очень просто определить типы полей структур.

Для float:

7ff78976360c **MOVSS** dword ptr [RDX + RCX\*0x1 + 0x40], XMM2

Далее надо опять вызвать мастер, в котором выбирать какие типы каким структурам присвоить, особенно в тех местах, где возник конфликт.

1. Зная оффсеты полей структур, их размеры, а также снимки объектов, можно потом точно определить типы.
2. Важно также определить типы полей-указателей! Для этого можно сохранять адреса объектов месте с их размерами, а также много снимков для каждого объекта. Потом на данном шаге сопоставлять поле-указатель по снимку с объектами из таблицы. В таблицу нужно будет заносить также список адресов!

Пример:

|  |  |  |
| --- | --- | --- |
| **Оффсет поля** | **Тип** | **Снимок** |
| 0x0 | Void\* | 0x7FF710120293 |
| 0x8 | int | 34, 78, 12, 33 |
| 0xc | float | 1.099, 2.33, … |
| 0x10 | Void\* | 0xba4455551 *-> class\_564* |

1. Распознать виртуальные таблицы

7ff789623a4b LEA **RAX**,[PTR\_LAB\_7ff78a3054a8] = *7ff7896247e0*

7ff789623a52 MOVSS XMM6,dword ptr [RSP + time]

7ff789623a58 XORPS XMM7,XMM7

7ff789623a5b COMISS XMM6,dword ptr [DAT\_7ff78a21d5a0]

7ff789623a62 MOV qword ptr [**R14**],**RAX**

7ff789623a65 MOV EAX,EBP

7ff789623a67 SETC AL

7ff789623a6a LEA RCX,[**R14** + 0xe0]

7ff789623a71 MOV RDX,RSI

7ff789623a74 MOVAPS xmmword ptr [**R14** + 0xb0],XMM7

7ff789623a7c MOV dword ptr [**R14** + 0xc0],EBP

7ff789623a83 MOV dword ptr [**R14** + 0xc4],EBX

Проходимся также по листингу, если видим присваивание по оффсету 0 некоторого статического адреса, то запоминаем это, т.е. заносим в таблицу. После анализа, когда мы прошлись по всем *конструкторам*, надо определить размер этих виртуальных таблиц.

Тут можно проходиться по всем функциям и делать поиск вирт. таблиц независимо, чтобы потом разграничить вирт. таблицы без использования гидры. Или можно юзать гидру и использовать разграничение по глобальным переменным. Лучше гидру, так как есть undefined функции. И вообще: пройтись по всем глобальным переменным. Если есть ссылка на функцию, то сделать из undefined обычную. Тогда можно хукнуть будет и их. И анализировать также.

Определить размер просто – идем вниз до тех пор, пока не встретим ссылку на другой конструктор. После этого создаем в сда объект виртуальной таблицы с функциями этими. Также у класса надо указать эту таблицу.

Потом можно в гидре самой сделать сигнатуры функций, тогда у нас виртуальные вызовы будут мало чем отличаться от невиртуальных -> больше определения типов.

Строки как пояснения к коду

Просмотр значений структур, визуализация координат

EXE and Libraries (DLL, Lib)

0x7FF7: GTA5.exe

0x7CD7: kernel32.dll

0x7AA7: d3d11.dll

Address space

Player\_GiveWeapon

Player\_SetSpeed

CreateFile

OpenFile

CreateD3D11Device

MSVRC.lib

rand

Есть единое адресное пространство процесса GTA5.exe. В нем расположены модули – это exe файл, а также динамические библиотеки. Статические библиотеки расположены внутри модуля GTA5.exe. Главный модуль – это исполняемый, все остальные обслуживают его и не могут работать независимо. Если посмотреть в стек, то первая функция – это main в .exe файле. Потом идем бесконечный цикл и в нем каждый кадр выполняются функции, вызовы которых образуют стек вызовов, причем вызов может быть библиотечной функции. Если функция принадлежит модулю динамической библиотеки, то команда call берет адрес функции из таблицы соотвествия.

Исполняемый модуль – агрегатор всех других модулей, которые вместе разделяют единое адресное пространство. Дочерние .exe не в счет, ибо у них другое пространство. У каждого модуля есть свой базовый адрес, относительно которого можно запомнить смещения функций и глобальных переменных.

В исходном коде программы DLL как и LIB предоставляют специальные .h файлы, в которых содержатся декларации функций. Реализации этих функций упакованы в самих модулях. Таким образом мы разделяем машинный код по разным файлам. Вызов библиотечной функции из программы – это ссылка на функцию, реализация которой в другом модуле.

Таким образом, DLL – это часть нашей программы, но просто физически она отделена от нее, но в исходниках нет. Это значит, что типы, классы и т.д.