**iOS静态检测API详细设计**

* com.bupt.ios.commonData

包功能简介：数据结构包，存放全局的变量

1. ProjectParameters

|  |  |
| --- | --- |
| 类名 | ProjectParameters |
| 功能 | 存放每次检测功能的参数 |
| ipaPath | 待检测ipa文件路径 |
| idaPath | IDA Pro路径 |
| detempPath | 反编译等逆向工作的根目录 |
| exeFilePath | ipa文件中可执行文件的路径 |
| idbPath | ida解析可执行文件生成的idb文件的路径 |
| idaPythonPath | 解析idb的python文件夹目录 |
| appName | ipa文件的名字 |
| reportPath | 最终报告生成路径 |

1. CommonData

|  |  |  |
| --- | --- | --- |
| 类名 | CommonData | |
| 功能 | 存放全局变量 | |
| rulePool1 | 简介 | 第一类规则库，存放解析后的第一类规则 |
| 类型 | List<SecRule> |
| addSecRule1 | 功能 | 添加一条规则 |
| 参数 | SecRule |
| getRulePool1 | 功能 | 获取规则库 |
| 返回 | List<SecRule> |

|  |  |  |
| --- | --- | --- |
| 类名 | CommonData | |
| 功能 | 存放全局变量 | |
| rulePool2 | 简介 | 第二类规则库，存放解析后的第二类规则 |
| 类型 | List<SecRule> |
| addSecRule2 | 功能 | 添加一条规则 |
| 参数 | SecRule |
| getRulePool2 | 功能 | 获取规则库 |
| 返回 | List<SecRule> |

* com.bupt.decompile

包功能简介：负责对ipa进行逆向反编译

1. IdaAnalyse

|  |  |  |  |
| --- | --- | --- | --- |
| 类名 | IdaAnalyse | | |
| 功能 | 调用IDA Pro分析ipa生成idb文件并分析 | | |
| genIDB() | 权限 | public：对外接口 | |
| 功能 | 调用IDA分析IPA生成IDB，并把文件转移到detemp/日期/ida下带解析 | |
| analyseIDB() | 权限 | private：内部方法 | |
| 功能 | 在genIDB中被调用，用于解析IDB文件 | |
| copy(Stirng soure, String des) | 权限 | private：内部方法 | |
| 参数 | String source | 源文件路径 |
| String des | 目的地址目录 |
| 功能 | 复制文件到指定目录 | |

1. UnzipIpa

|  |  |  |  |
| --- | --- | --- | --- |
| 类名 | UnzipIpa | | |
| 功能 | 解压IPA文件 | | |
| unzip(String filePath,String desDir) | 权限 | static public | |
| 参数 | String filePath | 待解压文件路径 |
| String desDir | 解压目录 |
| 功能 | 解压IPA文件 | |

1. VerifyEncryption

|  |  |  |  |
| --- | --- | --- | --- |
| 类名 | VerifyEncryption | | |
| 功能 | 判断可执行文件是否被加密 | | |
| Boolean  isEncryption (String filePath) | 权限 | public | |
| 参数 | String filePath | 可执行文件路径 |
| 功能 | 判断可执行文件是否加密 | |
| 返回值 | true：被加密  false：为加密 | |

* com.bupt.ios.scheduler

包功能简介：调度程序，包括整个程序的入口，负责工程多个功能模块的调度功能。

1. MainSheduler

|  |  |  |  |
| --- | --- | --- | --- |
| 类名 | MainScheduler | | |
| 功能 | 程序的入口，负责调度其他Scheduler | | |
| main(String [] arg) | 权限 | public static | |
| 参数 | 参数1 | IPA路径 |
| 功能 | 入口函数 | |

1. PreScheduler

|  |  |  |
| --- | --- | --- |
| 类名 | PreScheduler | |
| 功能 | 预处理 | |
| scheduler() | 权限 | public：对外接口 |
| 返回值 | boolean：预处理成功返回true |
| 功能 | 1. 初始化报告路径 2. 读取配置文件中的ida路径，并在ProjectParameter中set 3. 清空detemp文件，并生成当前分析缓存路径 |
| clearDetemp()  clearDir() | 权限 | private：内部方法 |
| 功能 | 清空detemp文件夹 |

1. AnalyseSheduler

|  |  |  |
| --- | --- | --- |
| 类名 | AnalyseScheduler | |
| 功能 | 解析调度器 | |
| scheduler() | 权限 | public：对外接口 |
| 功能 | 1. 判断ipa或者mach-o是否加密 2. 解压ipa 3. 定位可执行文件 4. 逆向ida生成idb并解析 |

* com.bupt.ios.rule

1. SecRule

|  |  |
| --- | --- |
| 类名 | SecRule |
| 功能 | 存放规则的数据结构 |
| ruleID(String) | 规则ID |
| ruleName(String) | 规则名称 |
| description(String) | 规则简介 |
| ruleType(int) | 规则类型：分为1和2。  1表示恶意API，匹配上规则表示存在漏洞  2表示保护API，没匹配上表示存在漏洞 |
| content(List<Function>) | 规则中需要匹配的API的列表 |
| riskLeve(int) | 危害等级 |
| solution(String) | 推荐的解决方案 |
| isEnable(boolean) | 是否启用规则。true启用 false禁用 |

1. Function

|  |  |
| --- | --- |
| 类名 | Function |
| 功能 | SecRule里面用到的API的数据结构 |
| FuncType (boolean) | API类型：分为true和false  最终SecRule匹配结果是SecRule里面每个API匹配结果相与得到，如果API类型为false，则API匹配结果取反，再同其他API匹配结果相与 |
| ClassName (String) | API需要匹配的类名，可以为“null” |
| FunctionName(String) | API名字，可以为“null” |
| Parameters (Map<String,String) | API的参数列表，类型是个Map，key是寄存器名称，value是参数的内容 |

1. ReadRules

|  |  |  |
| --- | --- | --- |
| 类名 | ReadRules | |
| 功能 | 读取规则文件，解析入库 | |
| readRules() | 权限 | public：对外接口  static：静态接口 |
| 功能 | 读取规则文件，判断规则文件是否启用，并根据规则类型，分别将规则添加到规则库1和2中 |

* com.bupt.ios.analyzer

1. IdaResultXmlParser

|  |  |  |
| --- | --- | --- |
| 类名 | IdaResultXmlParser | |
| 功能 | 解析IdaPython 的分析结果bl.xml，将bl.xml的内容存入IdaResultSet中 | |
| parseBlXml() | 权限 | public：对外接口  static：静态接口 |
| 功能 | 解析IdaPython 的分析结果bl.xml，将bl.xml的内容存入IdaResultSet中 |

1. BlMsg

|  |  |
| --- | --- |
| 类名 | BlMsg |
| 功能 | Ida汇编代码中bl的调用信息 |
| addr(String) | bl调用的地址 |
| name(String) | bl跳转的方法名 |
| regs(Map<String,String>) | bl跳转时的寄存器信息 |

1. IdaResultSet

|  |  |
| --- | --- |
| 类名 | IdaResultSet |
| 功能 | 存放bl.xml信息的数据结构 |
| MSG  Map<String, List<BlMsg>> | key：程序中的方法名  List<BlMsg>:该方法中的所有bl跳转信息 |

1. Analyzer

|  |  |  |
| --- | --- | --- |
| 类名 | Analyzer | |
| 功能 | 匹配规则(存于CommonData.rulePool1、CommonData.rulePool2)和IdaPython的解析结果(存于IdaResultSet.MSG) | |
| doAnalyzse() | 权限 | public：对外接口 |
| 功能 | 内部调用parsePool1()和parsePool2() |
| parsePool1() | 权限 | private：内部方法 |
| 功能 | 解析第一类规则 |
| 详情 | 1. 从规则池中选择一个规则 2. 从IdaResultSet中选择一个方法体 3. 从该规则中遍历每个规则方法 4. 针对每个规则方法，匹配IdaResultSet方法体中的每个Bl信息 5. 如果规则所有规则方法都匹配上，则规则命中，把规则和方法信息存入ReportSet.re1中 |
| parsePool2() | 权限 | private：内部方法 |
| 功能 | 解析第二类规则 |
| 详情 | 1. 从规则池中选择一个规则 2. 从IdaResultSet中选择一个方法体 3. 从该规则中遍历每个规则方法 4. 针对每个规则方法，匹配IdaResultSet方法体中的每个Bl信息 5. 如果规则所有规则方法都匹配上，则说明该规则安全，存入ReportSet.protectInfo；如果所有的IdaResultSet中的方法都没有匹配规则，则把规则信息存入ReportSet.re2 |
| cmpMap(Map<String, String>rule, Map<String, String>result) | 权限 | private：内部方法 |
| 功能 | 比较规则和bl信息中的寄存器内容是否匹配 |

* com.bupt.ios.report

1. ReportSet

|  |  |
| --- | --- |
| 类名 | ReportSet |
| 功能 | 存放规则信息匹配结果 |
| re1  Map<String, SecRule> | key：匹配上第一类规则的方法名  value:对应的规则信息 |
| re2  List<SecRule> | 未匹配上的第二类规则信息 |
| protectInfoMap  Map<String, SecRule> | key：匹配上第二类规则的方法名  value:对应的规则信息 |

1. WriteXml

* IDAPython

1. IDAPython.py

三个全局变量：

|  |  |
| --- | --- |
| 变量名 | regs |
| 类型 | 字典 Dictionary |
| 功能 | 针对每个方法，记录方法内部寄存器的状态，在解析每个方法前，会清空 |
| key | 寄存器名称，如X0，X1 |
| value | 寄存器内容 |

|  |  |
| --- | --- |
| 变量名 | msg\_send\_dict(弃用) |
| 类型 | 字典 Dictionary |
| 功能 | 每次调用msg\_send时，记录当前寄存器状态 |
| key | 当前方法名 |
| value | 类型是个List，List中的元素是regs |

|  |  |
| --- | --- |
| 变量名 | BL\_dic（弃用） |
| 类型 | 字典 Dictionary |
| 功能 | 针对除了msg\_send之前的API调用 |
| key | 被调用的API |
| value | 类型是个List，元素是API的调用者 |

|  |  |
| --- | --- |
| 变量名 | BL\_dic（改版） |
| 类型 | 字典 Dictionary |
| 功能 | 针对每个B或者BL调用时，寄存器信息 |
| key | Function Name （每个类中每个方法） |
| value | 类型是个List：  第一个元素是BL的方法名，如msg\_send；  第二个元素是BL指令的内存地址；  第三个元素是 一个dict：存入寄存器信息 |

关键方法

|  |  |
| --- | --- |
| 方法 | parseMOV |
| 传人参数 | addr：指令的地址 |
| 功能 | 解析当前的MOV指令 |

|  |  |
| --- | --- |
| 方法 | parseLDR |
| 传人参数 | addr：指令的地址 |
| 功能 | 解析当前的LDR指令 |

|  |  |
| --- | --- |
| 方法 | parseB |
| 传人参数 | addr：指令的地址 |
| 功能 | 解析当前的B系列的指令 |

|  |  |
| --- | --- |
| 方法 | parseSTR |
| 传人参数 | addr：指令的地址 |
| 功能 | 解析当前的STR系列的指令 |

|  |  |
| --- | --- |
| 方法 | parseOther |
| 传人参数 | addr：指令的地址 |
| 功能 | 解析当前其他指令 |

1. WriteBL

|  |  |
| --- | --- |
| 方法 | writeMsg |
| 传人参数 | BL\_dict：bl信息 |
| 功能 | 将IDAPython的解析结果存入bl.xml文件中 |