DR. Checker 污点分析部分阅读笔记

- 污点分析及检测器在 SSAPass 中注册并使用 （SoundyAliasAnalysis.cpp）
  - runOnModule 入口函数：146
    - 初始化，解析待分析的目标函数，进行别名分析等：173
    - 对待分析的目标函数，添加分析器（包括污点分析器），进行污点分析：195
- 污点分析器
  - **TaintAnalysisVisitor.cpp**
  - TaintedLoopBoundDetector.cpp
  - TaintedPointerDereference.cpp
  - TaintedSizeDetector.cpp
  - **Bug detector 和分析器的区别?**
- 基本分析器（GlobalVisitor.cpp）
  - 对各基本块使用分析器：287
  - 通过基类 InstVisitor 的方法 visit 基本块中的各条指令
    - **和 GlobalVisitor.h 里的 visit(BB) 没关系，因为 visit(BB) 不是 virtual 函数**
  - 使用各个分析器对各指令进行分析
    - **visitCallInst：分情况处理直接和间接函数调用**
      - 直接函数调用，直接通过 processCalledFunction 进行分析
      - 间接函数调用，获取可能的至多 5 个被调函数，通过 processCalledFunction 分别进行分析
    - processCalledFunction，103：创建并调用子函数的分析器
- 污点分析器（TaintAnalysisVisitor.cpp）
  - Visit 函数
    - visitAllocaInst：无操作
    - visitCastInst：把被 cast 的值的污点传播到该指令
    - visitBinaryOperator：将各操作数的污点传播到该指令
    - visitPHINode：将各操作数的污点传播到该指令
    - visitSelectInst：将各操作数的污点传播到该指令
    - visitGetElementPtrInst：将范围未被限制的 index 的污点传播到该指令
    - visitLoadInst：把 src 的污点信息和 src 指向的对象的污点信息传播到该指令
    - visitStoreInst：把 src 的污点信息传播到 dst 指向的对象
    - visitVAArgInst：未处理

- visitVACopyInst：未处理
- visitCallInst：分情况处理
  - Kernel 内部函数：进一步分情况处理
    - taint_initiator：将污点传播到函数参数指向的对象
    - memcpy_function：将 src 的污点传播到 dst
    - atoi_function：将字符串的污点传播到该指令
    - sscanf_function：将字符串的污点传播到各非格式化字符串的参数
  - 非 kernel 内部函数：为子函数建立上下文，并返回子函数污点分析器
- visitReturnInst：把返回值的污点信息记录到 retValTaints 中
- visitICmpInst：将各操作数的污点传播到该指令

- 辅助函数
  - getTaintInfo，26：从 currState 中找到当前上下文的污点 map，并从中取出对应值的污点信息
  - makeTaintInfoCopy，80：把 srcOperand 的污点信息 srcTaintInfo 传播到 targetInstruction，并在 dstTaintInfo 非空的时候也将污点信息传播到其中
  - updateTaintInfo，69：更新 currState 中存储的，当前上下文中 targetVal 的污点信息
  - mergeTaiintInfo，138：将 srcVals 中各值的各 TaintFlag 添加到 targetInstr 中
  - addNewTaintFlag，176：向 newTaintInfo 中添加 newTaintFlag（忽略重复元素）
  - setupCallContext，602：将形参中的污点信息传播到实参中
  - propogateTaintToArguments，500：将污点传播到函数参数指向的对象
  - propagateTaintToMemcpyArguments，658：将 src 的污点传播到 dst
  - getPtrTaintInfo，37：将 targetVal 指向的对象的污点返回到 retTaintFlag
  - **stitchChildContext，799：把子函数返回值的污点传播到函数调用指令**