需求设计说明书

项目名称：面向软件安全的污点数据检测系统

功能点：分析过程间的污点数据传播

项目成员：徐有健 欧锦荣 胡雄博 李珺

单位 : 南京大学计算机科学与技术系

**1** 引言

1.1 编写目的

本说明书用于说明污点数据在过程中是通过哪些方式传播的，预计跟踪规则以及在运行过程中可能遇到的故障和处理方法。具体内容包括软件结构，基本规则，协议约定，为软件设计和软件测试提供统一标准。

本说明书面向对象为*软件设计人员*以及*软件测试人员*。

使用对象：面向软件安全的污点数据检测研究整体项目组的其他项目成员。

1.2 背景

系统名称：面向软件安全的污点数据检测系统

项目任务提出者：华为公司

项目开发者：南京大学计算机系徐有健 欧锦荣 胡雄博 李珺

用户：软件开发者，维护者

单位：南京大学计算机系

背景介绍：

随着互联网和计算机软件的不断发展，软件的安全性问题得到了多方面的关注。攻击者会针对软件的漏洞进行恶意攻击，破坏软件的正确运行或获取非法的软件授权。因此，开发者们急需一种对软件进行漏洞检测（脆弱性测试）的高效准确的工具，根据检测修改代码，使软件在受到恶意攻击的情形下依然能够继续正确运行及确保软件被在授权范围内合法使用。所以该系统也要从污点数据检测研究开始做起，使得软件开发者和维护者能够高效的使用该系统来检测软件代码中的脆弱部分，以便进行优化。

1.3 参考资料

a．《软件工程：实践者的研究方法》Roger S. Pressman 著

b．软件文档规范及资料

**2** 任务概述

2.1 目标

1.根据上一模块，即判定污染源数据模块的结果，标记污染源

2.跟踪污染数据的传播路径，并检测出所有被传染得数据以及相关语句

3.对于跟踪污染源，编写系统调用的跟踪分析污点数据在过程间传播的模块代码

4.将检测结果汇总并提交至下一模块

2.2 用户的特点

规模较大的工程师团队，团队成员对于负责的设计有相应的水平，拥有较强的专业技术知识，但总体水平存在参差不齐的问题。

使用软件频度估计在1次/周到1次/月左右，每次使用允许软件运行5-6个小时。

2.3 假定和约束

假定：用户使用的开发语言稳定且代码规模不出现大的波动

约束：1. 污点数据传播的全面性约束

2. 项目的开发期限

3. 经费约束

**3** 用户描述

3.1 用户分类

软件开发者

软件维护者

软件测试者

3.2 用户说明

1. 软件测试者根据软件需求说明书对工程进行检测，根据运行结果进行汇总，评估测试结果并提供专业意见。
2. 软件开发者和软件维护者根据汇总结果检查代码段，参考测试意见对代码的薄弱处进行有效的代码改进，并对改进过的代码再次进行污点数据检测。

**4** 需求规定

4.1 对功能的规定

1. 要求对过程间的污点数据传播进行全面的分析，完成的模块代码能够正确的跟踪污点数据的过程间传播。允许使用者规定检测的粒度大小，以控制运行时间。
2. 对于给定的污染源能够判别出所有被该污染源污染的数据，并且判定语句是否具有污染检测的功能。若语句不具有污染检测的功能，则返回所在语句的位置

4.2对性能的规定

1. 时间特性要求：运行时间<12小时（基于通讯公司的情况）
2. 精确度：应精确到所在函数的行数

4.3输入输出要求

1. 输入：抽象的语法树，函数调用关系图，所有的过程信息，包括各个过程的参数以及返回参数

2. 输出：修改污染池中的内容，污染位置对应的代码行数，生成XML信息

4.4数据管理能力要求

要求有读取和存储过万行代码的能力。要求系统运行的硬件要求在合理范围内，系统维护污染池，必须控制污染池的大小。

4.5故障处理要求

1. 应对不同故障类型，自动选择跳过继续执行或者中止执行
2. 向用户发送错误报告，其中需要包含故障的种类，处理方法等信息。

5 运行环境规定

5.1 设备

应对不同的工程规模，设备要求不同，一般为普通PC

5.2 系统与软件要求

a.操作系统：各版本Linux系统

b.编译器及其他：Clang