

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

学号： 131220113

联系方式： tobuer2@126.com

单位： 南京大学计算机科学与技术系

目录

1 引言	3
1.1 编写目的.....	3
1.2 背景	3
1.3 参考资料.....	3
2 任务概述.....	3
2.1 目标	3
2.2 用户的特点.....	3
2.3 假定和约束.....	3
3 用户描述.....	3
3.1 用户分类.....	3
3.2 用户说明.....	4
4 需求规定.....	4
4.1 对功能的规定.....	4
4.2 对性能的规定.....	4
4.3 输入输出要求.....	4
4.4 数据管理能力要求.....	4
4.5 故障处理要求.....	4
5 运行环境规定.....	4
5.1 设备	4
5.2 支持软件.....	4

1 引言

1.1 编写目的

本说明书用于给出该总体项目中的分析程序运行间的污点数据传播过程的分析，给出了分析的目标。

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等

用户：软件开发者

实现软件单位：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. 分析过程间的污点数据传播情况
2. 和分析过程中的传播情况的项目组成员分类汇总各种传播情况
3. 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

2.2 用户的特点

系统使用者均为软件开发人员，拥有较强的专业技术知识。

2.3 假定和约束

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

软件开发者和维护者

3.2 用户说明

软件开发者和维护者使用该系统通过对污点数据传播的跟踪发现软件的薄弱点并加以改进。

4 需求规定

4.1 对功能的规定

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。

4.2 对性能的规定

1. 时间要求：要求整个系统运行时间不得超过 12 小时
2. 灵活性要求：允许同时在 Linux（Ubuntu）和 Windows 环境下运行

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，添加相应的污染位置

4.4 数据管理能力要求

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

允许保存系统的运行环境，使得可以在故障恢复后继续运行

5 运行环境规定

5.1 设备

PC

5.2 支持软件

- a. 操作系统
各版本 Linux 系统，最新版本的 Windows 系统
- b. 编译器及其他
Clang