软件安全入门

第七课 污点传播分析

目录

CONTENTS

01 污点传播分析基本原理

主要内容包括污点传播分析概述和主要分类、应用领域等。

污点分析是一种软件数据流分析技术，该技术通过将程序中的数据(外部输入数据或内部数据)标记为污点，跟踪程序处理污点数据的内部流程，**进而**帮助人们进行深入的程序分析和理解。

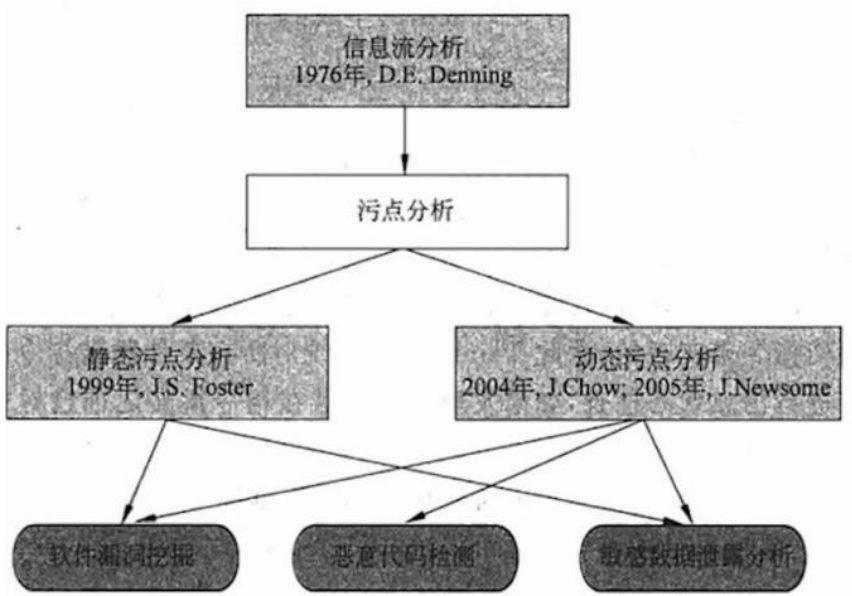


图 7-1　污点分析方法的发展及相关应用

动态污点分析在恶意代码检测、软件漏洞挖掘、敏感数据泄漏方面均取得了长足的发展。

1.恶意代码检测方面：大部分恶意代码往往需要依赖特定的外部数据作为攻击载体，通过污点分析来跟踪外部数据是否被用来作为某些异常行为的输入，可以有效检测蠕虫、木马等恶意代码。

2.软件漏洞挖掘方面：基于污点分析**的**智能型模糊测试方法相比传统的模糊测试，具备了数据格式以及程序行为语义的感知能力，避免了无效数据的生成，从而很大程度上提高了软件漏洞的挖掘效率。

3.敏感数据泄漏分析方面：运用污点分析技术可实现细粒度的敏感数据跟踪能力，分析其在程序运行时的实际处理过程，从而能够准确回答敏感数据是否存在被泄漏的可能。

1.首先需要确定污点源，即污点分析的目标来源，通常是程序外部(硬盘文件、网络数据等)的不可信数据或者用户所关心的程序内部数据。

2.随后利用传播规则(污点扩散、污点清除)计算所有涉及污点的执行过程。

3.最后进行污点检测。即在程序执行过程中的敏感位置(程序跳转、系统函数调用等)进行污点判断。

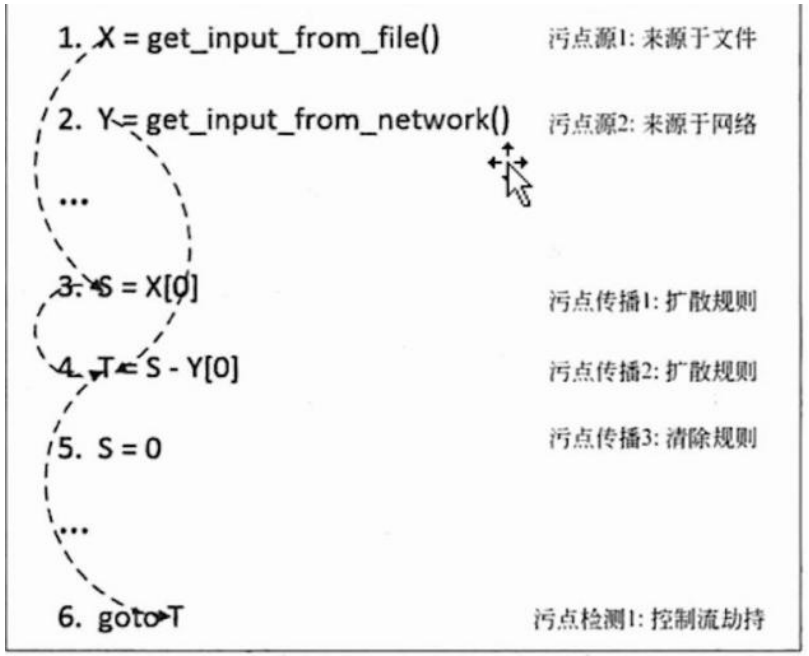


图 7-3 污点分析基本原理示例代码

02 污点传播分析主要方法

主要内容包括污点源识别、污点内存映射、污点动态跟踪等。

2.1 污点源识别

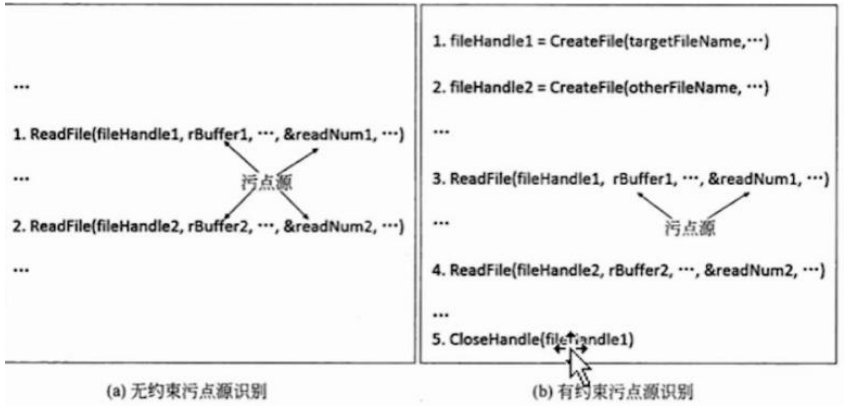
污点源识别方法主要分为两类：

1.无约束识别：即所有从外部读取的数据内容都作为污点源处理。

优点：简单直接；　缺点：带来较多的“污点噪音”导致分析效率降低。

2.有约束识别：即只有从特定文件或者网络地址读取的数据内容才作为污点源处理。

优点：能满足只对特定条件的数据进行跟踪；　缺点：需要监控较多的函数调用。



(a) 无约束污点源识别　(b) 有约束污点源识别

研究人员提出了一种记录数据的污点状态变化的方法—影子内存映射。主要分为两个阶段：映射过程和内存表示。其中，映射过程分为：

1.简单映射方法：为每一个污染的内存地址或者CPU寄存器额外分配一个内存映射空间。

优点：进行污点状态更新和查询时计算开销小。 缺点：需要预先分配较大的内存空间。

2.页表映射方法：使用一种类似页表映射的方法来实现影子内存。

优点：避免了简单映射的预先分配较大内存空间 缺点：污点分析过程中的分配开销较大

污点动态跟踪过程一般涉及三个阶段：

1.动态指令监控：也称动态指令插桩，基本原理是通过将程序加载到模拟CPU上运行，保证在程序每条指令或每个方法执行之前和之后可以提供相应的分析接口给用户，进而实现程序的动态分析。

2.污点传播计算：通过分析每条监控指令的语义信息，并利用相关的污点扩散、清除规则来保证正确的传播过程。

3.污点状态更新：反映传播计算的结果，一般通过更新影子内存来实现。影子内存更新的主要策略包括两类：一种是需要配合回溯分析的简单更新策略，一种是不需要回溯配置的多标签更新策略。

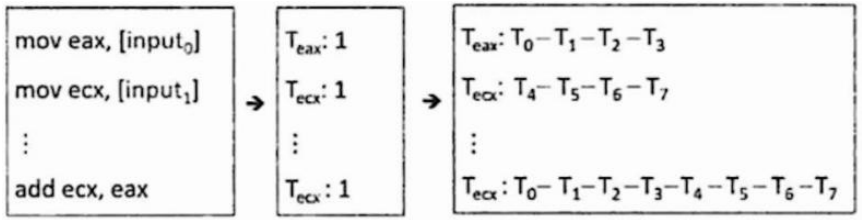


图 7-11　两种污点内存更新方式

主要内容包括TaintCheck系统、TEMU系统、AOTA系统。

TaintCheck是一套面向恶意代码自动检查、分析以及攻击特征生成的动态污点分析系统。其实现过程主要借助了二进制代码插桩工具Valgrind来实现程序的动态跟踪。

该系统主要由标记污染源的TaintSeed、跟踪污点传播的TaintTracker以及攻击发现的TaintAssert三个功能模块组成。

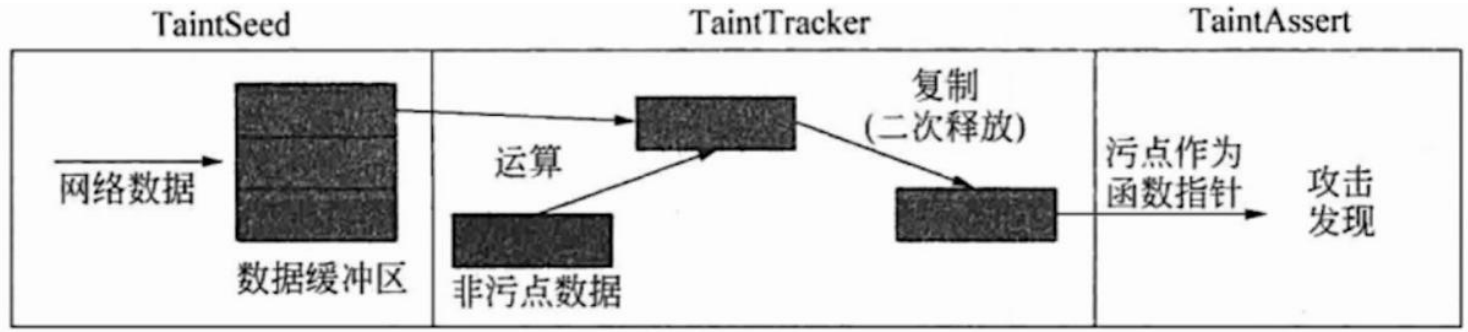


图 7-14　TaintCheck 系统组成

TEMU系统主要负责完成程序的动态分析任务。该系统在硬件模拟器QEMU的基础上实现了面向全系统跟踪的污点分析功能，同时实现了一套高可用的插件机制，能够快速构建面向不同应用领域的污点分析应用系统。

该系统由负责提取语义信息的系统语义提取模块、负责动态污点分析功能的污点分析引擎以及为用户提供丰富信息的插件机制组成。

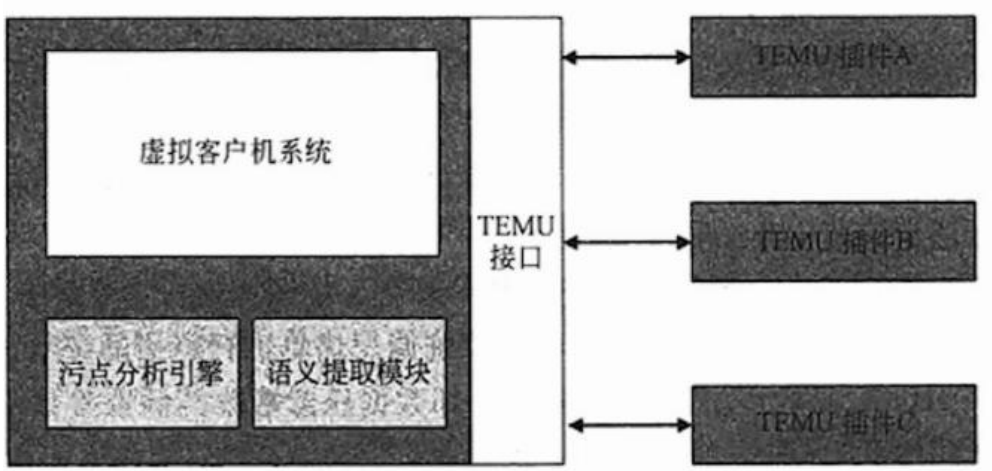


图 7-16　TEMU 系统组成

AOTA系统是中科院软件所搭建的一套面向Windows大规模应用程序的高实用性动态污点分析系统。该系统在硬件虚拟化平台上构建了完全透明的动态分析环境，并提供了离线或半在线污点分析，并构建了自动化分析与并行化分析过程。

该系统由负责操作系统语义的透明性分析的程序动态监控子系统、负责操作系统级的记录与重放的程序执行重放子系统以及负责动态污点分析的污点传播和回溯分析子系统组成。

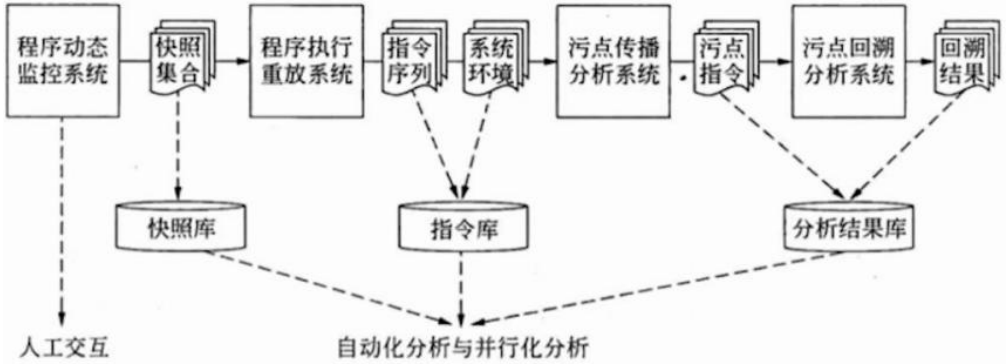


图 7-17　AOTA 系统组成

课程小结

•1.污点传播分析基本原理

·主要内容包括：污点传播分析概述和主要分类、应用领域等。

•2.污点传播分析主要方法

·主要内容包括：污点源识别、污点内存映射、污点动态跟踪等。

•3.典型系统实现

·主要内容包括：TaintCheck系统、TEMU系统、AOTA系统。

谢谢观赏