文章题目：基于静态插装和约束求解的整数漏洞检测

作 者：张帆,张聪,徐明迪,杨捷

发表刊物：华中科技大学学报

（一）阅读概述：

此篇文章以二进制程序的Ｃ源码为研究对象，通过静态插装和符号执行的手段对整数漏洞进行检测．作者提出的技术实现如下:

①在Ｃ源码中可能的整数漏洞点前面插装检测代码。

②定位可能导致整数漏洞的输入源，并将其标记为符号变量。

③将静态插装后的源码编译成可执行代码，并进行符号混合执行。

④在动态执行的过程中，通过对插装代码对应的符号约束进行求解，可以检测整数漏洞是否存在，以及获得当整数漏洞存在时符号变量相应的具体取值。

⑤通过对从程序入口点到整数漏洞点所经过路径上的所有条件跳转约束进行求解，获得引导程序到达整数漏洞点时符号变量相应的具体取值．结合两者可以辅助生成触发漏洞的输入用例。

（二）文章结构

0.前言

介绍了现阶段的整数漏洞的挖掘方法，比较了相关研究（但比较浅）

１.Ｃ语言中的整数漏洞及程序插装

1.1 Ｃ语言中的整数漏洞

针对整数漏洞类型和存在原因进行了阐述，并对整数漏洞挖掘的相关技术进行了分析和研究。

1.2 Ｃ语言中整数操作的操作语义

作者自身定义了一些函数规则。

1.3 针对不安全整数操作的程序插装

提出了插桩，但并未做详细的阐述。

２.Ｃ语言中整数溢出漏洞检测

2.1 源程序符号标记与插装

2.2 运行时符号执行和约束求解

从配置文件中读取不可信的整数输入源（ｓｏｕｒｃｅ）和脆弱性检测点（ｓｉｎｋ）．配置文件主要由分析人员手工指定最可能导致整数漏洞的不可信整数输入源，以及最可能存在整数漏洞的高危整数操作点插装增强的程序在运行过程中，通过符号执行和约束求解对整数漏洞是否存在进行判定，以及存在时生成测试用例的过程。

2.3 整数脆弱点定位

３.实验验证（略）