《计算机系统基础实践》任务书

# 实验二 机器级语言理解——二进制炸弹拆除

**一、实验目的与要求**

通过逆向分析一个二进制程序（称为“二进制炸弹”）的构成和运行逻辑，加深对理论课中关于程序的机器级表示各方面知识点的理解，增强反汇编、跟踪、分析、调试等能力。

实验环境：Ubuntu，GCC，GDB等

**二、实验内容**

**任务1** 二进制炸弹拆除

“二进制炸弹”是一个 Linux 可执行程序。每个同学按自己学号，到群文件中下载自己的压缩包，解压后可得到bomb执行程序和bomb.c总控源程序。

bomb执行程序由六个阶段组成。每个阶段都需要输入特定的字符串。如果输入了正确的字符串，那么该阶段就“解除”。 否则，炸弹会通过打印“BOOM！！！”。每个同学的目标是解除尽可能多的阶段。

进度提示：

本实验使用两次课内上机，8学时完成。找出尽可能多的密码字符串。

**三、实验提示**

每个同学的“解除”字符串也会不同。每个炸弹阶段会测试不同的方面：

第1阶段：字符串比较

第 2 阶段：循环

第 3 阶段：条件/开关

第 4 阶段：递归调用和堆栈规则

第 5 阶段：指针

第 6 阶段：链表/指针/结构体

还有一个“秘密阶段”，仅当学生将特定字符串附加到第四阶段时才会出现。

为了拆除炸弹，学生必须使用调试器，通常是gdb反汇编执行文件，并单步执行每个阶段的机器代码，使用课程中的知识来推断“解除”字符串。

还可以使用objdump工具，将bomb执行程序静态反汇编，通过研读生成的源程序，理解和掌握bomb的执行过程。objdump反汇编得到源程序的命令为：

objdump -d bomb > bomb.s