二进制代码漏洞自动挖掘与利用系统

黄桦烽、和亮、杨轶、苏璞睿、徐鹏、余媛萍

联系方式（黄桦烽　huafeng@iscas.ac.cn）

具体内容介绍

1. **系统简介：**该系统针对二进制程序进行漏洞自动挖掘、分析和利用，基于模糊测试技术进行漏洞自动挖掘，基于污点分析技术反馈生成模糊测试样本和对崩溃样本初步分析筛选可利用样本，最后基于输出反馈调节及符号执行对输入进行求解。

2. **功能指标:**
   - ◆ 支持二进制程序的自动化模糊测试
   - ◆ 支持字节粒度的高效精准动态污点传播分析
   - ◆ 支持控制流劫持、格式化字符串、系统调用后门等类型漏洞的自动判定和利用生成

3. **方法创新：**提出基于程序运行时的漏洞描述模型，通过脆弱性和污点属性对漏洞进行定义和描述，该模型支持漏洞挖掘、分析、利用过程中对漏洞进行统一描述，形成了一体化的框架。

4. **技术优势：**该系统应用到2018年DEFCON China大会BCTF比赛，在99秒内完成第一个漏洞自动挖掘和利用，在2分48秒内完成了4个样本的自动利用，而人类战队完成第一个漏洞利用花了17分钟，获得了机器人自动攻防单项排名的第一的成绩。