A Survey of System Fuzzing

Abstract: 【200～250】模糊测试现在已经发展成为一种高效的漏洞挖掘方法，符号执行也是当前流行的软件漏洞挖掘技术，两者都是网络与信息安全领域的研究热点。混合模糊测试是在传统模糊测试的基础上加入了符号执行技术，目前已经发展成为模糊测试的新分支。文章对现有的混合模糊测试方法进行研究，综述了混合模糊测试的发展演变过程和技术核心，并通过一种基于符号执行的实验方法对目前知名的混合模糊测试进行性能对比。最后讨论了目前混合模糊测试领域研究存在的问题，并尝试对其未来发展趋势进行了展望。

Key Words：混合模糊测试、模糊测试、符号执行、覆盖率

1. Introduction【600～650】
2. 技术概述【850内】

2.1. Fuzzing

2.2. System Fuzzing

1. 研究现状【1700内】

【按照分类进行以及分类，按照时间线进行类别下排序】

1. Further Directions【550～600】
2. Conclusions【250～300】

Reference【28～30】