北京工业大学

毕业设计（论文）任务书

题目 基于二进制动态翻译的 ROP 攻击检测方法研究与实现

专业 _____ 学号 _____ 姓名 _____

主要内容

1、 ROP 攻击及其变种攻击检测方法设计

通过对 ROP 攻击及其变种攻击的特点进行归纳总结，设计和实现一种基于二进制动态翻译的 ROP 攻击及其变种攻击的检测方法，利用二进制动态插桩框架 PIN 或其他工具实现 ROP 攻击的检测策略、JOP 攻击的检测策略、return-into-libc 攻击等的检测策略，及最终的攻击检测效果的实现，从而实现完整的 ROP 攻击及其变种攻击的检测过程。

2、 ROP 攻击检测方法实现

实现一个检测 ROP 攻击、JOP 攻击及 return-into-libc 攻击的程序，能够检测出 ROP 攻击及其变种攻击，并发出相应的警告。

3、 ROP 攻击检测系统测试

根据上述工作完成基于 B/S 模式实现 ROP 攻击及其变种攻击检测方法的界面展示。

基本要求

1、 掌握 ROP 攻击原理，总结 ROP 攻击及其变种攻击的特点

2、 掌握二进制插桩框架 PIN 的使用

3、 完成 ROP 攻击检测方法的设计、实现和测试，编写相关文档

主要参考资料

[1] Si L., Yu J., Luo L., Ma J., Wu Q., Li S. (2016) ROP-Hunt: Detecting Return-Oriented Programming Attacks in Applications. In: Wang G., Ray I., Alcaraz Calero J., Thampi S. (eds) Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2016. Lecture Notes in Computer Science, vol 10066. Springer, Cham

[2] Shacham H.The geometry of innocent flesh on the bone: return-into-libc without function calls (on the x86) [C] // proc of the 14th ACM Conf on Computer and Communications Security. New York: ACM,2007:552-561

完成期限：2019.6

指导教师签章：_____

专业负责人签章 _____