北京工业大学学生开题报告表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课题名称 | 基于二进制动态翻译的ROP攻击检测方法研究与实现 | | | | |
| 课题来源 |  | 课题类型 | CX | 导 师 | 詹静 |
| 学生姓名 | 刘天祺 | 学 号 | 15074707 | 专 业 | 物联网工程 |
| 开题报告内容：  在开题前，我对即将研究的题目进行深入的调查，熟悉并掌握了相关的背景知识，并且完成了一篇相关论文的翻译工作，与此同时，我查阅了与ROP攻击相关的十余篇文章，增进我对该领域及我所研究的题目的理解。  目前的ROP攻击防御机制可粗略分为5种：1.控制流完整性检测；2.动态/静态指令检测；3.用户输入扫描；4.指令重构；5.内存随机化。我所设计的题目属于第二类中的动态指令检测，即：在程序运行时动态地检测指令，并根据获取的信息判断程序行为是否为ROP攻击。  我设计本方案的目的在于检测并防御ROP攻击，在程序遭到ROP攻击时及时关闭程序，防止损失。设计的要求是防御现有的各种ROP攻击及其变种，并且不误报，以免影响程序的正常工作。我目前的思路是结合静态和动态检测，选取恰当的ROP特征对其进行识别。结合静态分析的原因在于，动态检测会导致程序放缓，为了减少检测带来的这种副作用，我决定引入静态分析，利用静态分析获取尽可能多的信息，从而减少动态检测时获取的信息量以达到整体优化的目的。我预期达到的结果是：取得尽可能小的系统开销。  任务完成的阶段内容及时间安排如下：  任务内容：  - 1.查阅资料，了解ROP攻击及其变种，并归纳总结其特点。  - 2.查阅资料，了解现有的ROP攻击及其变种的检测方法。  - 3.熟悉动态插桩工具PIN的使用方法。  - 4.设计ROP攻击及其变种检测的新方案并实现。  - 5.通过界面展示攻击检测结果。  时间安排：  - 2018.12 – 2019.3 完成工作前两项，查阅资料，加深对课题的理解。  - 2019.3 – 2019.4 开题，提出检测方案。初步实现并不断优化检测方案。  - 2019.4 – 2019.5 优化、调试程序，撰写论文。  我本科期间曾参加过信息安全类的竞赛，专攻二进制安全。在此期间，我积累了丰富的攻防经验，熟悉linux环境以及各种调试工具的使用，对程序编译的各个环节以及一些常见漏洞的原理有深入理解。我认为我可以完成本课题中的任务。望予批准开题。 | | | | | |

课题类型：（1）A—工程设计；B—技术开发；C—软件工程；D—理论研究；

（2）X—真实课题；Y—模拟课题；Z—虚拟课题

（1）、（2）均要填，如AY、BX等。