ROP-Hunt：在应用程序中检测返回导向编程(ROP)攻击

摘要:

返回导向编程(ROP) 是一种新型漏洞利用技术，该技术通过重复使用已有的小代码序列(gadget)构造出一条gadget链，从而执行任意的非法操作。尽管很多防御机制已经被提出，但是一些新的ROP攻击的变种能够轻易绕过这些机制防御。

在本文中，我们将介绍一个新工具ROP-Hunt，它能依据正常程序与恶意ROP代码间的差异来防御ROP攻击。ROP-Hunt利用it\*技术并在程序运行时检测ROP攻击。在我们的实验中，ROP-Hunt可以在众多真实例程中检测出所有类型的ROP攻击。我们使用了几个原版的SPEC2006标准来测试ROP-Hunt的性能，结果表明它具有零误报率和可接受的系统开销。