ROP: definition, defense, and variations

Song Young Iek, Yoon Kyoung Taek, Lee ga gi

Abstract—Rop is considered as one of the effective ways of attack in Information Security. We will explain about ROP's definition and why it was made. Then we will mention defense methods such as Position-Independent Executable(PIE), Stack canarie. Finally we will discuss briefly about ROP's four variations:Jump oriented Programming(JOP),String Oriented Programming(SOP),Blind Return oriented programming(BOP),Signal Return Oriented Programming(SOP)

Index Terms—ROP, Position-Independent Executable(PIE), Stack canarie, Jump oriented Programming(JOP),String Oriented Programming(SOP),Blind Return oriented programming(BOP),Signal Return Oriented Programming(SOP)

1 Introduction

In the early history of Information Security, most of the attacks were using buffer overflow bug. exploiting buffer-overflow try to control the program counter by injecting your shellcode in memory. Make program counter register to point your shellcode program. However, as Information Security techniques were developed to countermeasure buffer overflow attack, such as Non eXecute bit : Add Nx bit in hardware level. It raises exception if CPU tries to execute something that doesnt have NX bit. Nx bit is located and setup in page table. Make memory sections like stack,heap non-executable. Make it impossible to execute injected shellcode by buffer overflow ASLR(Address Space Layout Randomization) : Map heap and stack at random location. In order to overcome these kinds of defense, attackers developed an ROP attack.

2 Requirement