Address Space Layout Randomization

Derek Rosario

Context

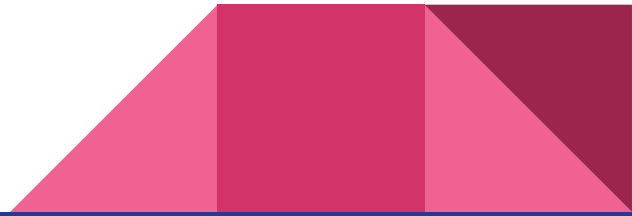
- Many possible ways to exploit a system
  - Side-channel attacks
  - Buffer Overflows
  - Other Memory Vulnerabilities

- Need: Preventative measures for such attacks
  - Or, at the very least, stuff to mitigate the attack in the event that an exploit does occur

Why DEP Doesn’t Cut It

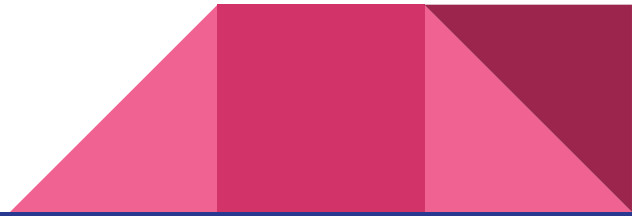
- Data execution prevention: a software + hardware enforced mechanism that prevents the execution of code in a non-executable memory location
  - Prevents code from being executed on the stack, heap, etc.
  - First introduced in Windows XP Service Pack 2; also in Mac OS and Linux

- In short: ROP beats DEP



ASLR

- Randomizes the location of executables in memory, such as:
  - The main program itself
  - The call stack
  - The heap
  - Any dynamic libraries being used
  - Memory-mapped files
  - Data structures used in the application
  - Etc.
- Idea: an attack needs to be specifically tailored to the process space at the time in which this data is randomized for the attack to have any effect.



Implementation(s)

- When should things be randomized?
  - Linux ASLR vs. OS X ASLR
- What should be randomized?
  - In other words, how aggressive should the randomization be?
- How much of the virtual address space should be used for this?
  - Very few implementations make use of the full virtual memory space for randomization

Limitations

Performance:

- Really only feasible on more powerful devices
- Compatibility Issues
- How do you randomize growable objects?

Security:

- Doesn’t trap the attack
- No information provided
- Not actually that robust

Sources

Marc-Gisbert, Hector; Ripoll R. Ismael. Address Space Randomization Next Generation

Jang, Yeongjin; et. al. Breaking Kernel Address Space Layout Randomization with Intel TSX

Shacham, Hovav; et. al. On the Effectiveness of Address Space Randomization

Thompson, Jacob. Six Facts About Address Space Randomization on Windows

Xu, J; Kalbarczyk, Z; Iyer, R. Transparent runtime randomization for security