

➡ Position Independent Executables





➡ Non-exhaustive. Often implemented at OS or Compiler

Exploit Mitigation Contd.

Exploit Mitigation Contd.

- ➡ Position Independent Executables
- ➡ Control Flow Guard
- ➡ Application sandboxing
- ➡ Non-exhaustive. Often implemented at OS or Compiler

Fortify Source Functions

- ➔ GCC macro `FORTIFY_SOURCE` provides buffer overflow checks for unsafe C libraries

`memcpy, memcpy, memmove, memset, strcpy, stpcpy, strncpy, strcat, strncat, sprintf, vsprintf, snprintf, vsnprintf, gets`

Checks are performed

- some at compile time (compiler warnings)
- other at run time (code dynamically added to binary)