Mitigations

- Patching
- Data Execution Prevention
- Address Space Layout Randomization
    - To make it harder for buffer overruns to execute privileged instructions at known addresses in memory.
- Principle of Least Privilege
    - Eg running Internet Explorer with the Administrator SID disabled in the process token. Reduces the ability of buffer overrun exploits to run as elevated user.
- Code Signing
    - Requiring kernel mode code to be digitally signed.
- Compiler Security Features
    - Use of compilers that trap buffer overruns.
- Encryption
    - Of software and/or firmware components.
- Mandatory Access Controls
    - MACs
    - Access Control Lists (ACLs)
    - Operating systems with Mandatory Access Controls - eg. SELinux.
- Insecure by Exception
    - When to allow people to do certain things for their job, and how to improve everything else. Don't try to "fix" security, just improve it by 99%.
- Do Not Blame the User
    - Security is about protecting people, we should build technology that people can trust, not constantly blame users.