Buffer Overrun

Buffer Overrun

- A program writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory.
- C and C++ provide no built-in protection against accessing arrays.

Buffer Overrun

- If the buffer overrun goes over the end to the data segment in a program, this results in a segmentation fault and core dump.
- If not, the error can sometimes be exploited by an attacker.
- Stack and Heap based Exploitation.

Stack Based Exploitation

- Change the values of nearby variables.
- Change the value of the return address.
  - To the address of a user input buffer
  - which can contain a program.

Safety

- Libraries exist for safe manipulation of buffers.
- Buffer overflow protection is used to detect the most common buffer overflows by checking that the stack has not been altered when a function returns.
- If it has been altered, the program exits with a segmentation fault.

Safety

- Three such systems are
  - Libsafe
  - *StackGuard*
  - *ProPolice* gcc patches.