UNIVERSITY OF OREGON

# CIS433/533 - Computer and Network Security

# Software Security

Professor Kevin Butler
Winter 2010

# Buffer Overflow

UNIVERSITY OF OREGON

- Very common attack mechanism
  - from 1988 Morris Worm to Code Red, Slammer, Sasser and many others
- prevention techniques known
- still of major concern due to
  - legacy of widely deployed buggy
  - continued careless programming techniques

# Buffer Overflow Basics

UNIVERSITY OF OREGON

- caused by programming error
- allows more data to be stored than capacity available in a fixed sized buffer
  - buffer can be on stack, heap, global data
- overwriting adjacent memory locations
  - corruption of program data
  - unexpected transfer of control
  - memory access violation
  - execution of code chosen by attacker