Prevention Systems: IDs with a hammer

buffer overflow
- If you declare a var that holds 6 chars and you write 10
  - you either error or write over memory
- Big issue in C & C++ because of memory management
- Python and Java are safer but slower
- But in time compilers look ahead
- Where?
  - basically everywhere
  - seg fault
  - crash immediately
- If you're doing a service it could cause DoS
- Stack smashing (read contents of stack and overwrite)
- What's on stack: return address, local variables
Java has immutable strings
C doesn't
- Protect
  - input side
  - copying values
  - How do you know what's exact?
  - no opt: steal (slide down to code you don't to start executing)
- Heap
  - mmu can mark something as read only
Help ourselves
  - memory address space
  - random placement (performance cost)
  - swap pages
  - Canaries (check if air is bad)
  - Stack guard
was a huge effort to firm it up to lessen vulnerability
boot were lazy