P193-197

- 指针
  - 数组与指针紧密联系着
  - 将指针容一种类型强转成另一种类型，则只改变类型，而不改变其值。比如 char *p，值为 p，那么表达式（int *）p + 7 则等于 p + 28
  - 指针也可以指向函数：比如：

```
int fun(int x, int *p);
```

然后，我们可以声明一个指针 fp，将它赋值为这个函数，代码如下：

```
int (*fp)(int, int *);
fp  = fun;
```

然后用这个指针来调用这个函数：

```
int y = 1;
int result = fp(3, &y);
```

- 内存越界引用和缓冲区溢出
  - c 语言对数组不进行任何边界检查，局部变量和状态信息都保存在栈中。而如果对越界数组元素的写操作，必然会破坏栈中的信息，引发一系列错误
  - 比如**缓冲区溢出。**对抗方式：
    - 栈随机化。使分配的栈地址不连续，给出一定的溢出容忍度
    - 栈破坏检测。