

规格严格 功夫到家



第8章 指针

——指针变量的定义、初始化及解引用



哈尔滨工业大学

苏小红 sxh@hit.edu.cn

本节要讨论的主要问题

- 变量的寻址方式哪有几种?
- 何为指针?如何定义指针类型的变量?
- 如何访问指针变量指向的存储单元中的数据?



指针

- 指针(Pointer)是"稀饭(C Fans)"最挚爱的武器
- C的高效、高能主要来自于指针
- 很多 "Mission Impossible"由指针完成
 - * 大多数语言都有无数的"不可能"
 - * 而C语言是
 - □ "一切皆有可能" ——
 - □ "Impossible is Nothing" ——



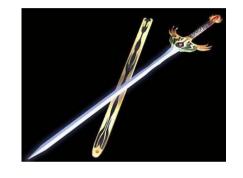




指针



强转与指针,并称C语言的两大神器用好了可呼风唤雨,威力无比用不好也会伤及自身



屠龙刀





倚天剑

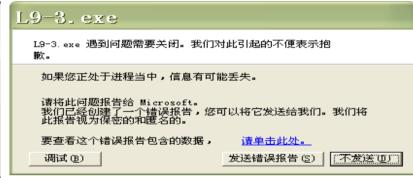
指针

- 是谁惹的祸?
 - 几乎全是由指针和数组引起的非法内存访问导致的
- 黑客攻击服务器利用的bug绝大部分都是指针和数组造成的



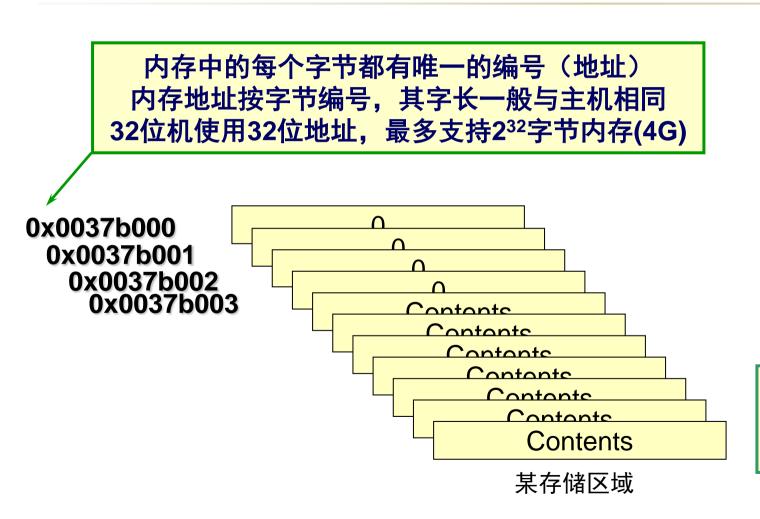


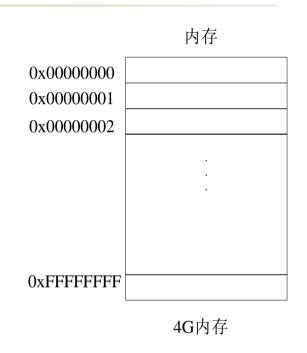




■ 理解指针要从变量的地址谈起

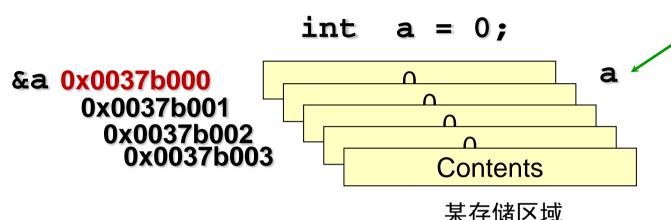
内存如何编址?





地址是一个无符号整数,从0开始,依次递增。在表达和交流时,通 常把地址写成十六进制数

如何对变量进行寻址?

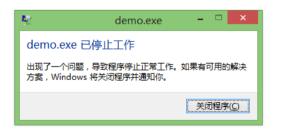


直接到变量名标识的存储单元中 读取变量的值——直接寻址

某存储区域

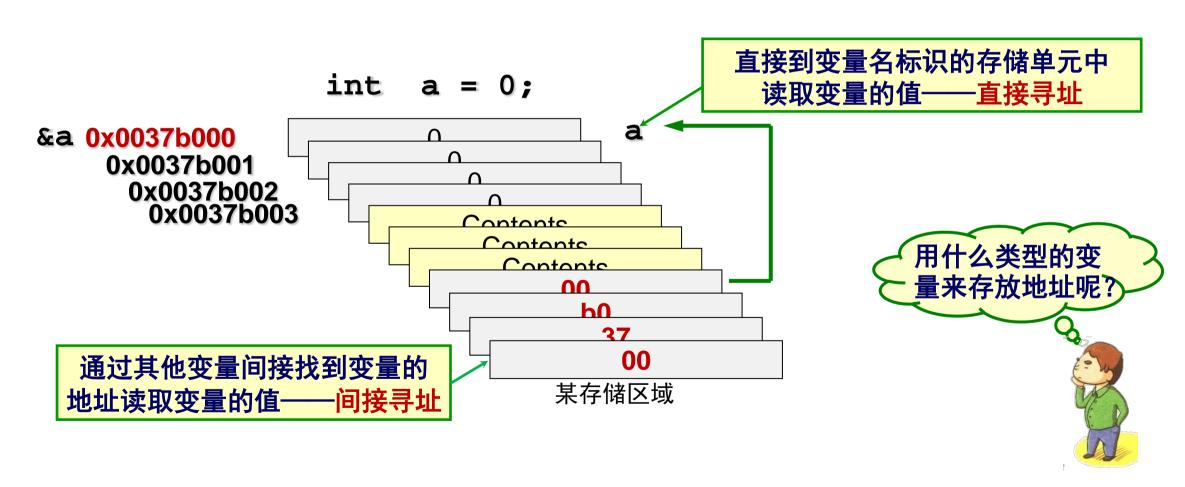
#include <stdio.h> int main() int a = 0; scanf("%d", a); printf("a=%d\n", a); return 0;

问题:输入数据时忘记使用取地址运算符&,这样会如何?



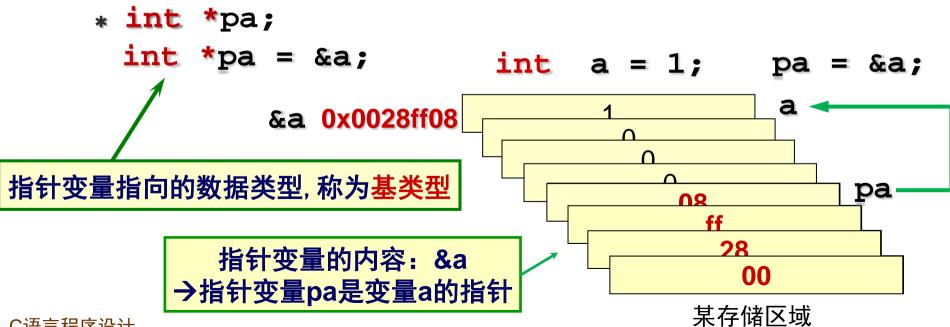
a的值被当作地址。如a值为 100,则输入的整数就会从 地址100开始写入内存

如何对变量进行寻址?



用什么类型的变量来存放变量的地址?

- 指针(Pointer)类型
- 指针变量——具有指针类型的变量
 - * 保存32位地址值——sizeof(pa)是4个字节
 - * 用什么数据类型去理解它所指向的存储单元中的数据呢?



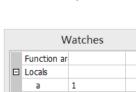


如何显示变量的地址?

■ 使用%p格式符

```
#include <stdio.h>
int main()
  int a = 0;
  int *pa;
  printf("a=%d\n", a);
  printf("&a=%p\n", &a);
  printf("pa=%p\n", pa);
  return 0;
```





0x28ff0c

指针变量只能指向同一基类型的变量

```
#include <stdio.h>
int main()
  int a = 0;
  int *pa = &a;
  printf("a=%d\n", a);
  printf("&a=%p\n", &a);
  printf("pa=%p\n", pa);
  return 0;
```

使用未初始化的指针会怎样?

- 指针变量使用之前必须初始化
- 若你不知把它指向哪里,那就指向NULL(在stdio.h中定义为0)

```
#include <stdio.h>
int main()
  int a = 0;
  int *pa;
  printf("a=%d\n", a);
  printf("&a=p\n", &a);
  printf("pa=%p\n", pa);
  return 0;
```

```
warning: 'pa' is used uninitialized
```

```
#include <stdio.h>
int main()
{
  int a = 0;
  int *pa = NULL;
  .....
  return 0;
}
```





NULL是什么?

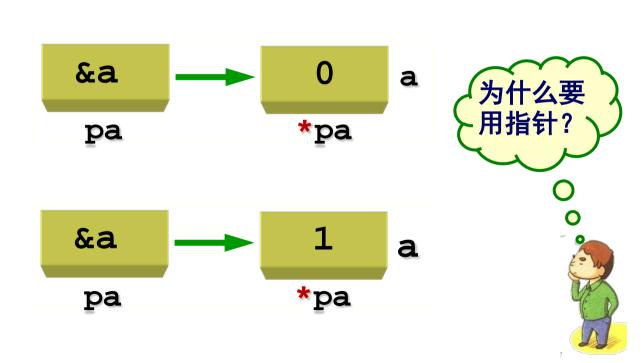
- 空指针—值为NULL的指针,即无效指针
- 问题: p = 0 和 p = NULL 有什么区别吗?
 - * p = NULL可以明确地说明p是指针变量,而不是一个数值型变量
- 问题:空指针就是指向地址为0的存储单元的指针吗?
- 答案: 不一定
 - * 并非所有编译器都使用0地址
 - * 某些编译器为空指针使用不存在的内存地址



如何访问指针变量指向的存储单元中的数据?

- 通过间接寻址运算符访问(引用)指针变量指向的变量的值
- ——指针的解引用(Pointer Dereference)

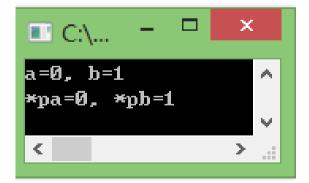
```
#include <stdio.h>
int main()
  int a = 0;
  int *pa = &a;
  *pa = 1;
  printf("a=%d\n", a);
  printf("*p=%d\n", *pa);
  return 0;
```



指针变量的定义和初始化

```
#include <stdio.h>
int main()
  int a = 0, b = 1;
  int *pa, *pb;
  pa = &a;
  b = dg
  printf("a=%d, b=%d\n", a, b);
  printf("*pa=%d, *pb=%d\n", *pa, *pb);
  return 0;
```

不能写成: int* pa, pb;



讨论

■ 国际C语言混乱代码大赛(IOCCC)要求参赛者写出最有创意的最让人难以理解的C语言代码,并限制在4 kilobytes以内。第20届IOCCC获得最佳展示奖的是 Don Yang的作品(详细说明地址 http://www.ioccc.org/2011/akari/hint.html)。对于这样的大赛及其获奖作品,你怎么看?

```
*/ #include<stdio.h>
                       /*2w0,1m2,] <n+a m+o>r>i>=>(['0n1'0)1;
                    */int/**/main(int/**/n,char**m)(FILE*p,*g;int
                  #uinndcelfu dset<rsitcdti oa.nhs>i/ */;char*d="P%"
                 "\n$d\n\nnwh+" h[1024] v[]="vmrivmrarararavmrnvmri*daijiken**akkari~n**"
         "/y*u*k/riin<ty(uyr)g,aur,arr[a1r2a82*y2*/u*r{uyu}ri0cyurhiyua**rrar+*arayra*='
       "yuruyurwiyuriyurara'rariayuruyuriyuriyu>rarararayuruy9uriyu3rivurar aBrMaPrOaWv^?'
      "*]/f]`;hvroai<dp/f*i*s/<ii(f)a{tpquat<cahfaurh(+uf)a;f}vivn+tf/q*`*w/jmaa+i`ni("/**
     */"i+k[>+b+i>++b++>1[rb";int/**/u;for(i=0;i<101;i++)y[i*2]^="~hktrvq~dmG*eoa+%squ#12"
     ":(wn\"11))v?wM353{/Y;lgcGp`vedllwudvOK`cct~[|ju {stkjalor(stwvne\"gt\"yogYURUYURI"[
     i]^y[i*2+1]^4;/*!*/p=(n>1&&(m[1][0]-'-'||m[1][1] !='\0'))?fopen(m[1],y+298):stdin;
      /*y/riynrt~(^w^)],]c+h+a+r+*+*[n>)+{>f+o<r<(-m]
                                                       =<2<5<64;}-]-(m+;yry[rm*])/[*
       */q=(n<3||!(m[2][0]-'-'||m[2][1]))?stdout /*]{
                                                        }[*/:fopen(m[2],d+14);if(!p||/*
       "]<<*-]>y++>u>>+r >+u+++y>--u---r>++i+++" <)<
                                                          "for\40%sing\n",m[!p?1:2],!p?/*
   return+printf("Can " "not\x20open\40%s\40" ""
                                                           &-1.9-2-)-|-|.28>-w-?-m.:>([28+
 o=82]5<<+(+3+1+&.(+ m +-+1.)<)<|<|.6>4>-+(> m-
 */"read": "writ");for ( a=k=u= 0;y[u]; u=2 +u) {y[k++ ]=y[u];}if((a=fread(b,1,1024/*
                              R*/ )>/*U{ */ 2&& b/*Y*/[0]/*U*/="P' &&4=/*"y*r/y)r\}
,mY/R*Y"R*/,p/*U*/)/*
*/sscanf(b,d,&k,& A,&
                                               ! (k-6&&k -5) &&r==255) {u=A; if (n>3) {/*
1&<1<6<?<m.-+1>3> +:+ .1>3+++
                                               -;.u+=++.1<0< <; f<o<r<(.;<([m(=)/8*/
                                               >>1,i>>1,r);u = k-5?8:4;k=3;}else
u++;i++;}fprintf (q, d,k,
 /*]>*/{(u)=/*{ p> >u >t>-]s
                                                               n+14>17) ?8/4:8*5/
                                               >++(.vrvr*/+(
    4:)for(r=i=0 : :)(n*=6:n+=
                                                (n>3?1:0):if
                                                               (v[n]&01) fonte(/
      <q-e<t.c>h.a r -(-).)8+<1.</pre>
                                                              <)+{+i.f>([180*/1*
     (r),q);if(y[u ]&16)k=A;if
                                                              (v[n]&2)k--:if(i/*
      ("^w^NAMORI: { I*/==a/*"
                                                             )*/){/**/i=a=(u)*11
       &255;if(1&&0>=
                                                            fread(b,1,1024,p)) &&
       ")]i>(w)-;} {
                                                            /i-f-(-m--M1-0.)<{"
        [ 8]-59/* */
                                                           )break; i=0; }r=b[i++]
           :u+=(/**>>
                                                         *..</<<)<[[;]**/+8&*
           (y+u))?(10-
                                    r?4:2):(y[u]
                                                        &4)?(k?2:4):2;u=y[u/*
            49;7i\(w)/;}
                                    y}ru\=*ri[
                                                       ,mc]o;n}trientuu ren (
             */]-(int)''';}
                                                       p);k= +fclose(q);
             /*] <*.na/m*o{ri{
                 */ return k-
                    ( -/*}/ */0x01
                                       /*^w^*/
```





