Security holes and Virus

- Security holes
- Virus

写课程感想

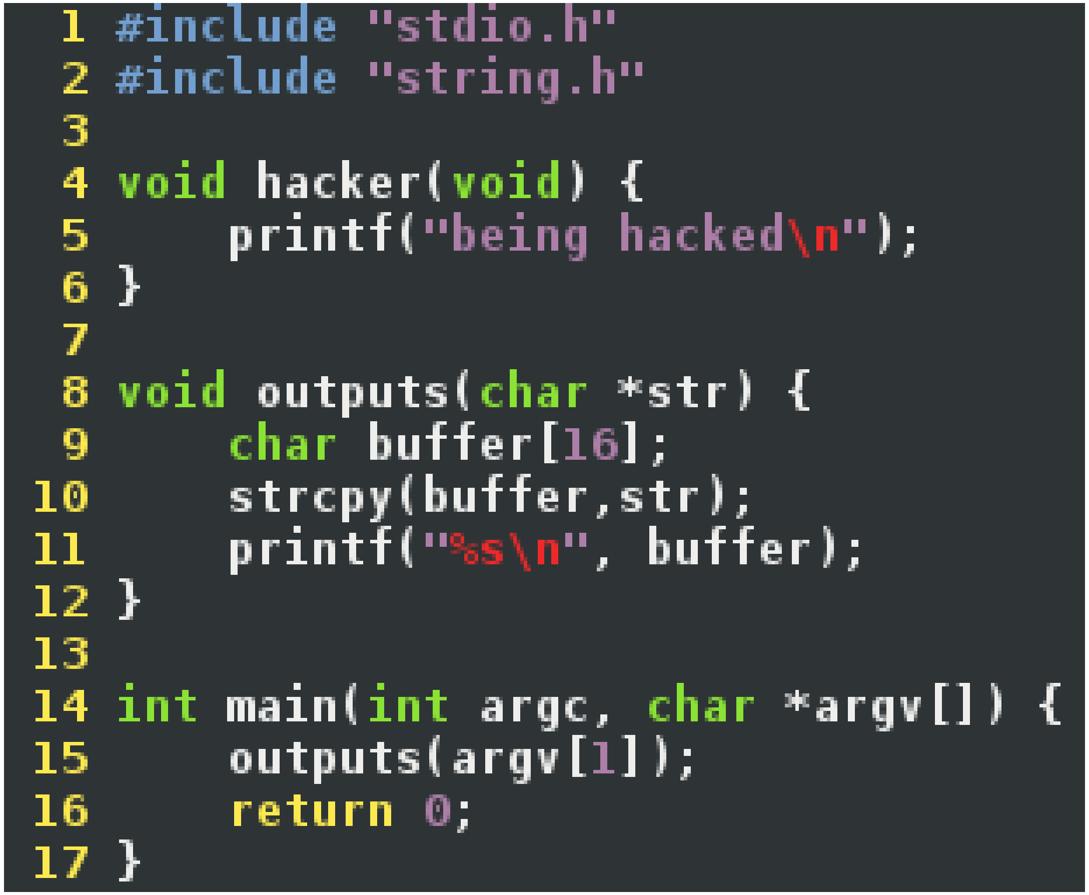
- 提交地址
  - ftp://172.25.46.144/upload/lab4
  - co_jd_stu
  - txt文件，文件名随机
    - 文件中不出现个人信息
- 内容
  - 收获，反思，建议，吐槽...
  - 我看(也可以写一些理论课感想)
  - 若不想写，请写“无感想”并提交
- 全体加分
  - 认真写 > “无感想” > 不提交 > 造假
- Due date – 2014/06/15 23:59:59

- Security holes

Software vulnerabilities

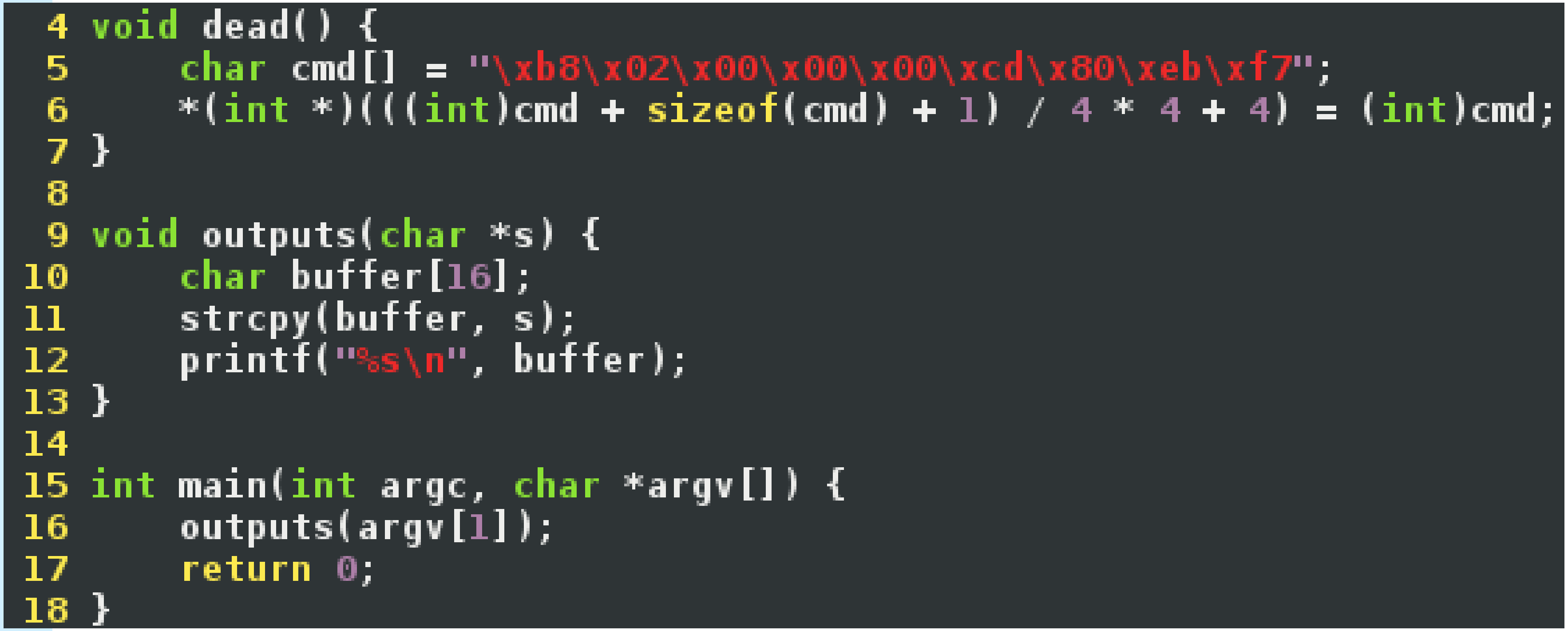
- The attacker can do something that he should not have rights to.
- types
  - Memory safety violations
  - Input validation errors
  - Race conditions
  - Privilege-confusion bugs
  - Privilege escalation
  - ...
- We will explore some of them.

Buffer overflows



```c
#include "stdio.h"
#include "string.h"

void hacker(void) {
    printf("being hacked\n");
}

void outputs(char *str) {
    char buffer[16];
    strcpy(buffer,str);
    printf("%s\n", buffer);
}

int main(int argc, char *argv[]) {
    outputs(argv[1]);
    return 0;
}
```

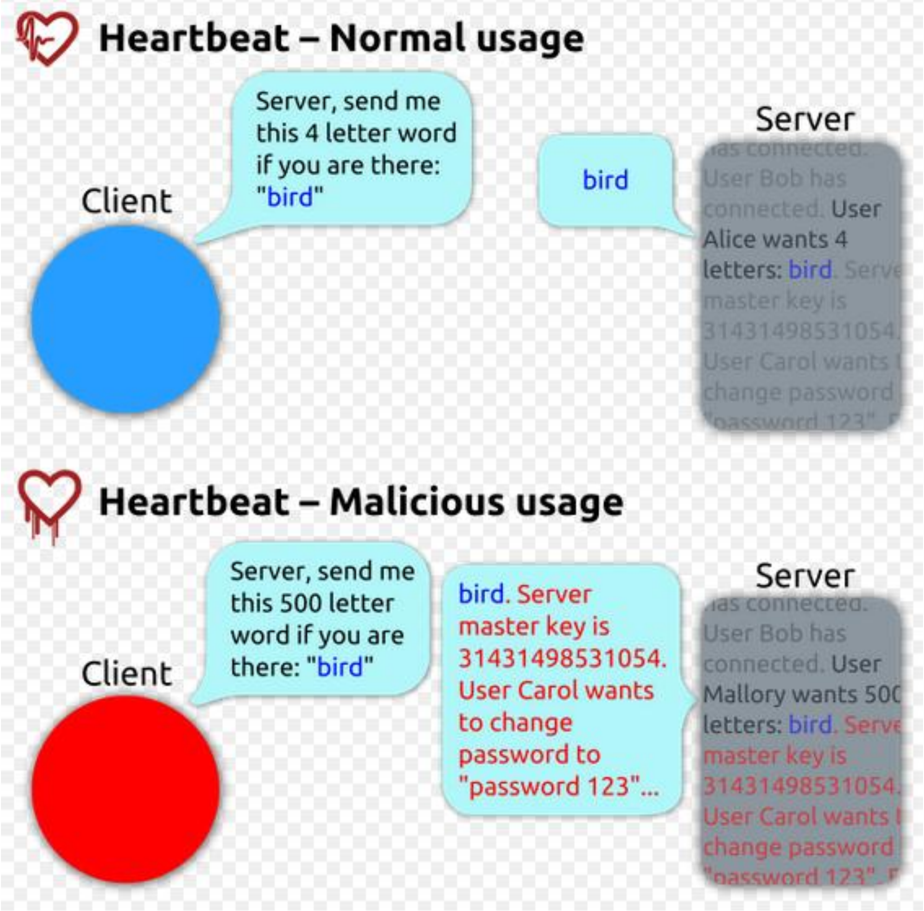
Buffer overflows



```c
void dead() {
    char cmd[] = "\xb8\x02\x00\x00\x00\xcd\x80\xeb\xf7";
    *(int *)(((int)cmd + sizeof(cmd) + 1) / 4 * 4 + 4) = (int)cmd;
}

void outputs(char *s) {
    char buffer[16];
    strcpy(buffer, s);
    printf("%s\n", buffer);
}

int main(int argc, char *argv[]) {
    outputs(argv[1]);
    return 0;
}
```

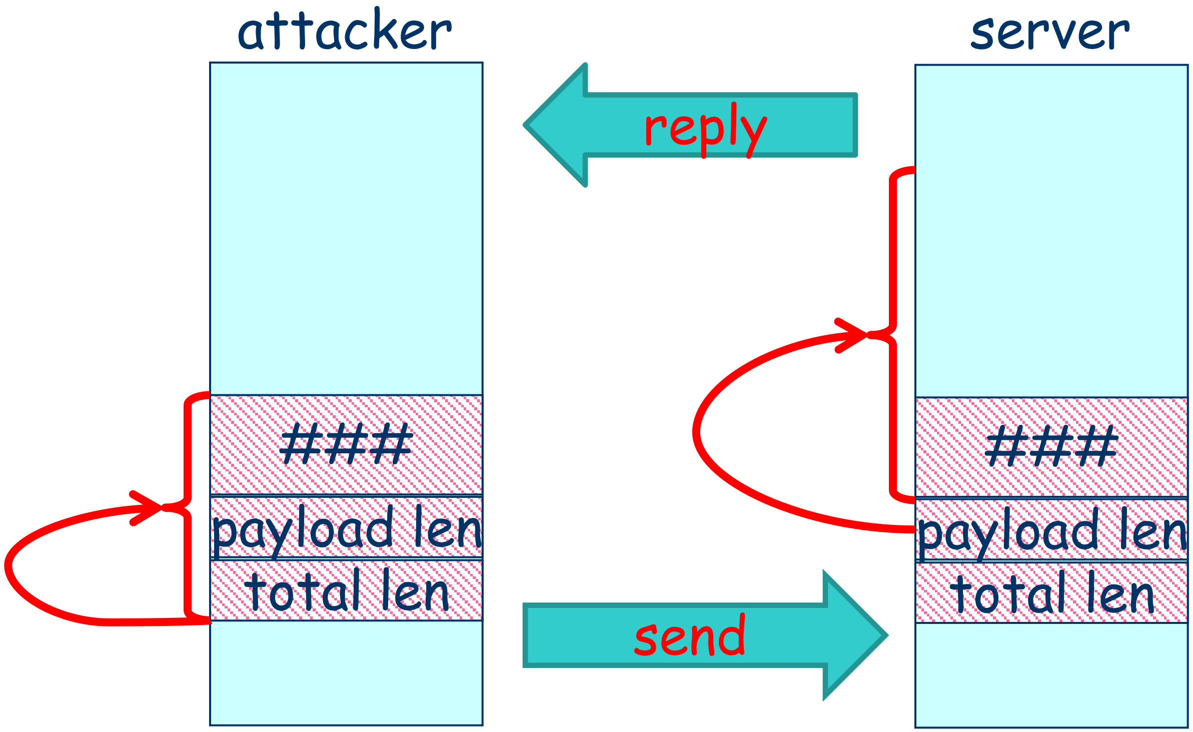
Buffer over-read

- OpenSSL hearbeat security hole


Heartbeat – Normal usage
Client
Server, send me this 4 letter word if you are there: "bird"
bird
Server
has connected. User Bob has connected. User Alice wants 4 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". F
Heartbeat – Malicious usage
Client
Server, send me this 500 letter word if you are there: "bird"
bird. Server master key is 31431498531054. User Carol wants to change password to "password 123"...
Server
has connected. User Bob has connected. User Mallory wants 500 letters: bird. Serve master key is 31431498531054. User Carol wants t change password "password 123". F

OpenSSL security hole

- variable-length message



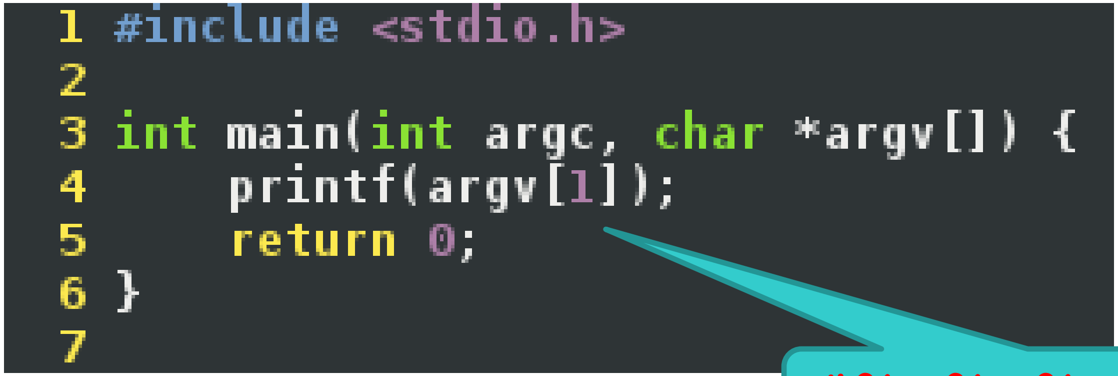
OpenSSL - code simulation

http://www.myhack58.com/Article/60/63/2014/44763.htm

```
int main() {
  char other1[100] ;memset(other1,'E',100);
  char package_send[plen_real] = {0xF,'d','a','t','a'};//获得的数据包
  char other2[100] ;memset(other2,'E',100);
  char* pdata = package_send+1;
  int plen_fake = package_send[0];
  char* package_return = (char*)malloc(plen_fake +1 );//新数据包
  memcpy(package_return+1, pdata, plen_fake);

  printf("package data send:\n");
  for(int i = 1;i<plen_real;i++) printf("%c",package_send[i]);
  printf("\n");
  printf("package data send back:\n");
  for(int i = 1;i<plen_fake +1;i++) printf("%c",package_return[i]);
  printf("\n");

  return 0;
}
```

```
package data send:
data
package data send back:
dataEEEEEEEEEEE
```

Format string attacks



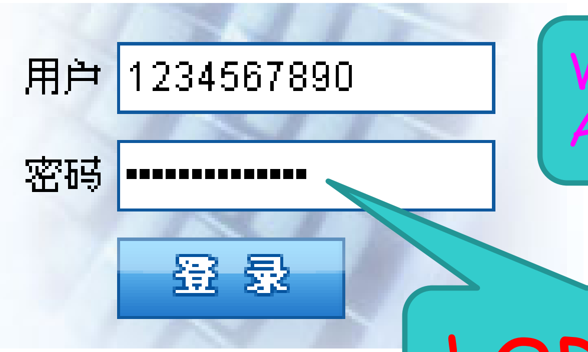
```c
#include <stdio.h>

int main(int argc, char *argv[]) {
    printf(argv[1]);
    return 0;
}

```

"%x%x%x%x%x"

- print contents in the stack
  - execute command
  - environment variables

Code injection

```
SELECT *
FROM UserList
WHERE UserList.Username = 'Username'
AND UserList.Password = 'Password'
```

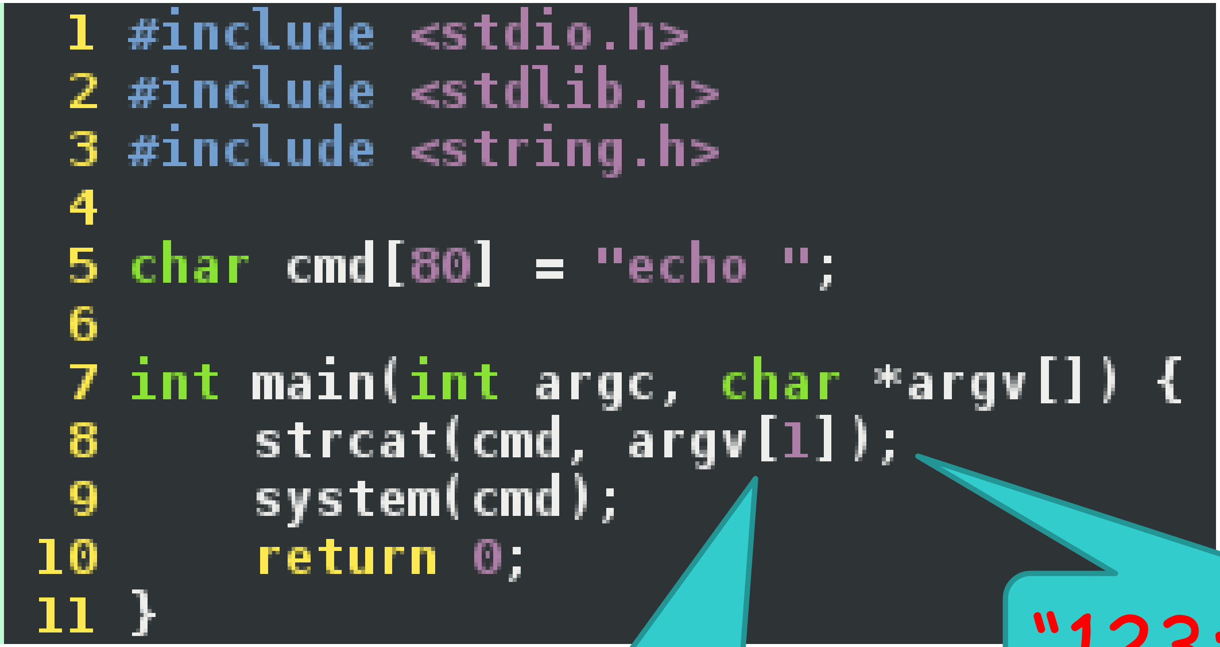


用户 1234567890

```
WHERE UserList.Username = 'Username'
AND UserList.Password = '' OR '1'='1'
```

' OR '1'='1

Code injection



```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

char cmd[80] = "echo ";

int main(int argc, char *argv[]) {
      strcat(cmd, argv[1]);
      system(cmd);
      return 0;
}
```

“123; echo abc”

“bye; :(){ :|:& };:”

Directory traversal attack

```
<?php
$template = 'red.php';
if (isset($_COOKIE['TEMPLATE']))
   $template = $_COOKIE['TEMPLATE'];
include ("/home/users/phpguru/templates/" . $template);
?>
```

```
GET /vulnerable.php HTTP/1.0
Cookie: TEMPLATE=../../../../../../../../../etc/passwd
```

```
HTTP/1.0 200 OK
Content-Type: text/html
Server: Apache

root:fi3sED95ibqR6:0:1:System Operator:/:/bin/ksh
daemon:*:1:1::/tmp:
phpguru:f8fk3j1OIf31.:182:100:Developer:/home/users/phpguru/:/bin/csh
```

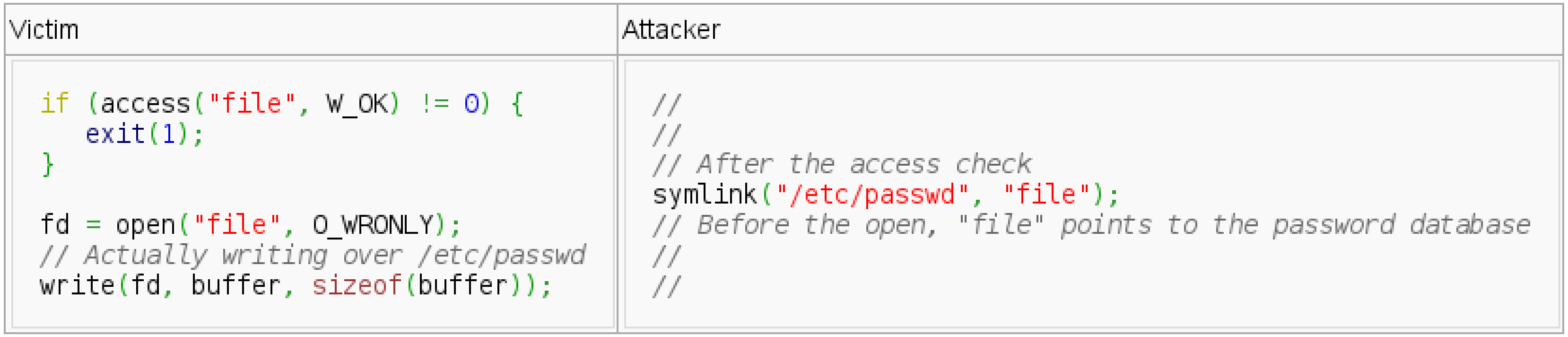
Cross-site request forgery

- browsing a chat forum

```
Mallory: Hello Alice! Look here:
   <img
src="http://bank.example.com/withdraw?account=
Alice&amount=1000000&for=Mallory">
```

- Alice's bank keeps her authentication information in a cookie
- The cookie hasn't expired

Time of check to time of use



<table>
<tr><th>Victim</th><th>Attacker</th></tr>
<tr><td><pre>
if (access("file", W_OK) != 0) {
   exit(1);
}

fd = open("file", O_WRONLY);
// Actually writing over /etc/passwd
write(fd, buffer, sizeof(buffer));
</pre></td><td><pre>
//
//
// After the access check
symlink("/etc/passwd", "file");
// Before the open, "file" points to the password database
//
//
</pre></td></tr>
</table>

- The state managed by the OS may change between system calls.

Symlink race

```
fd = open("/tmp/passwd");
// ...
write(fd, buf, sizeof(buf));
// ...
remove("/tmp/passwd");
```

```
symlink("/tmp/passwd", "/tmp/a");
```

- How to keep the content of "passwd"?
- create a symbol link /tmp/passwd ➔ /tmp/a
  - open("/tmp/passwd") ➔create file "a"
  - write(fd, buf, sizeof(buf)) ➔ write to file "a"
  - remove("/tmp/passwd") ➔ remove link "passwd"

Performance holes

```
h = zend_inline_hash_func(arKey, nKeyLength);
nIndex = h & ht->nTableMask;
p = ht->arBuckets[nIndex];
if (p != NULL) {
    // collision
}
```

Performance holes

```
$size = pow(2, 15);

$array = array();
for ($key = 0, $maxKey = ($size - 1) * $size;
$key <= $maxKey; $key += $size) {
    $array[$key] = 0;
}
```

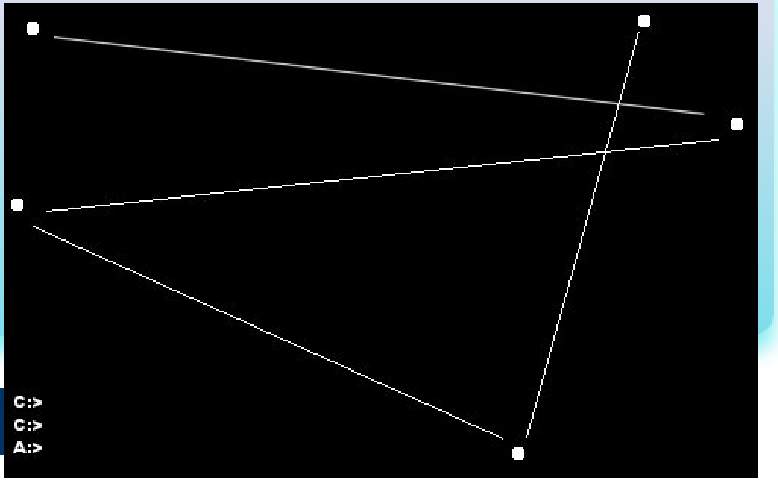
- 0.035s → 59.7s

- Virus

Jerusalem(黑色星期五) Virus (1987)

- .EXE files grow by 1,808~1,823 bytes each time they are infected.
- hooks itself into interrupt processing and other low level DOS services
  - suppress console messages
    - "Bad command or file name"➔"Bad Command or file name"
- On Friday 13th, it deletes every program file that was executed.
- DOS ➔ Windows

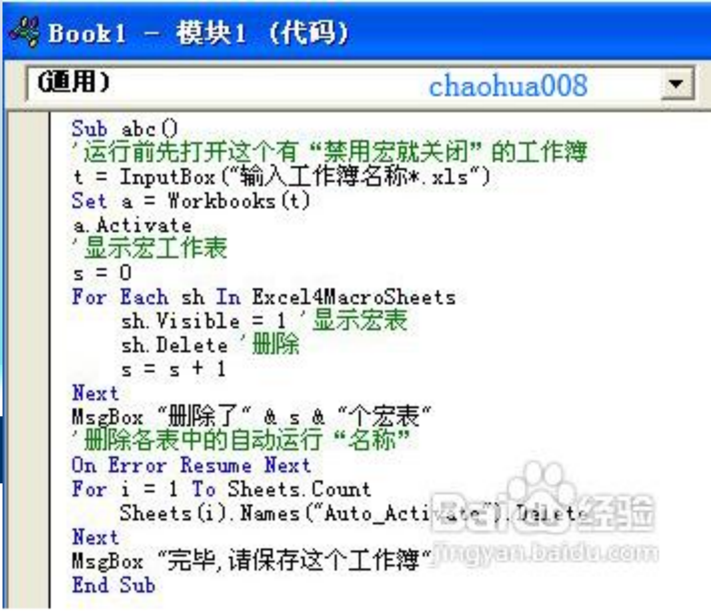
Ping-Pong Virus (1988)



```
C:>
C:>
A:>
```

- boot sector virus
- protect by labeling itself as 1 KB bad cluster in a floppy disk
- disk access on the half hour → show a small "ball" bouncing around the screen
- crash when running on 386 machine
  - cause by “MOV CS,AX" instruction
- Can you implement it?

Macro virus (1996)

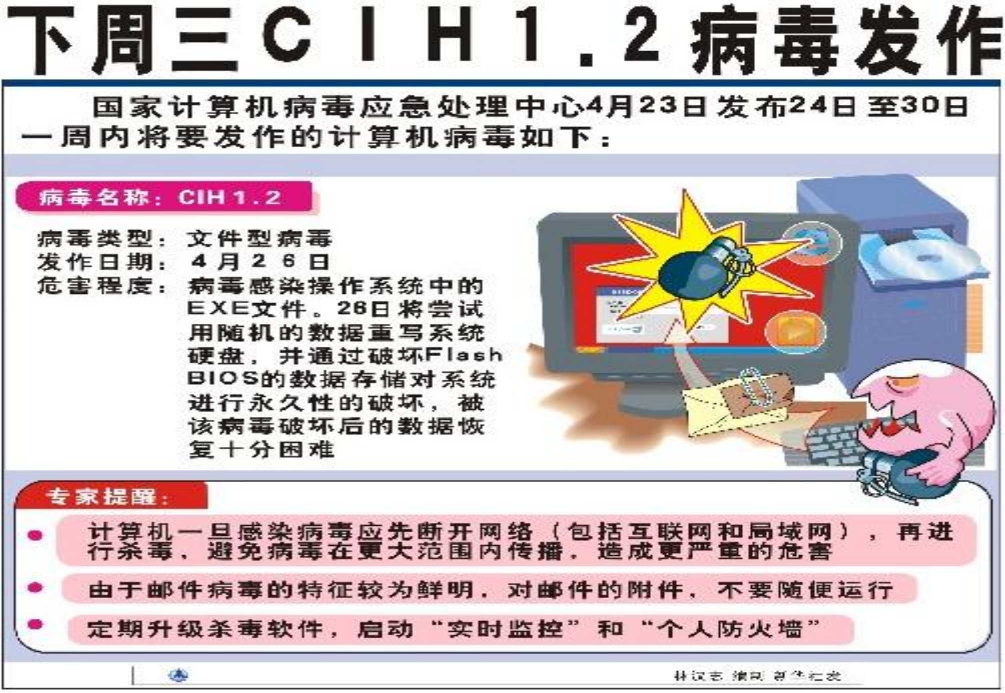


```
Sub abc()
'运行前先打开这个有“禁用宏就关闭”的工作簿
t = InputBox("输入工作簿名称*.xls")
Set a = Workbooks(t)
a.Activate
'显示宏工作表
s = 0
For Each sh In Excel4MacroSheets
    sh.Visible = 1 '显示宏表
    sh.Delete '删除
    s = s + 1
Next
MsgBox "删除了" & s & "个宏表"
'删除各表中的自动运行“名称”
On Error Resume Next
For i = 1 To Sheets.Count
    Sheets(i).Names("Auto_Activate").Delete
Next
MsgBox "完毕,请保存这个工作簿"
End Sub
```

Baidu经验
jingyan.baidu.com

- spread through e-mail attachments, disks, networks...
- embed itself in other documents and templates
- corrupt other parts of the system, depending on what resources a macro can get access to
- Melissa(1999)
  - The virus would then send itself by email to the first 50 people in the person's address book.

CIH (1998)



下周三CIH1.2病毒发作

国家计算机病毒应急处理中心4月23日发布24日至30日一周内将要发作的计算机病毒如下：

病毒名称：CIH1.2

病毒类型：文件型病毒
发作日期：4月26日
危害程度：病毒感染操作系统中的EXE文件。26日将尝试用随机的数据重写系统硬盘，并通过破坏Flash BIOS的数据存储对系统进行永久性的破坏，被该病毒破坏后的数据恢复十分困难

专家提醒：

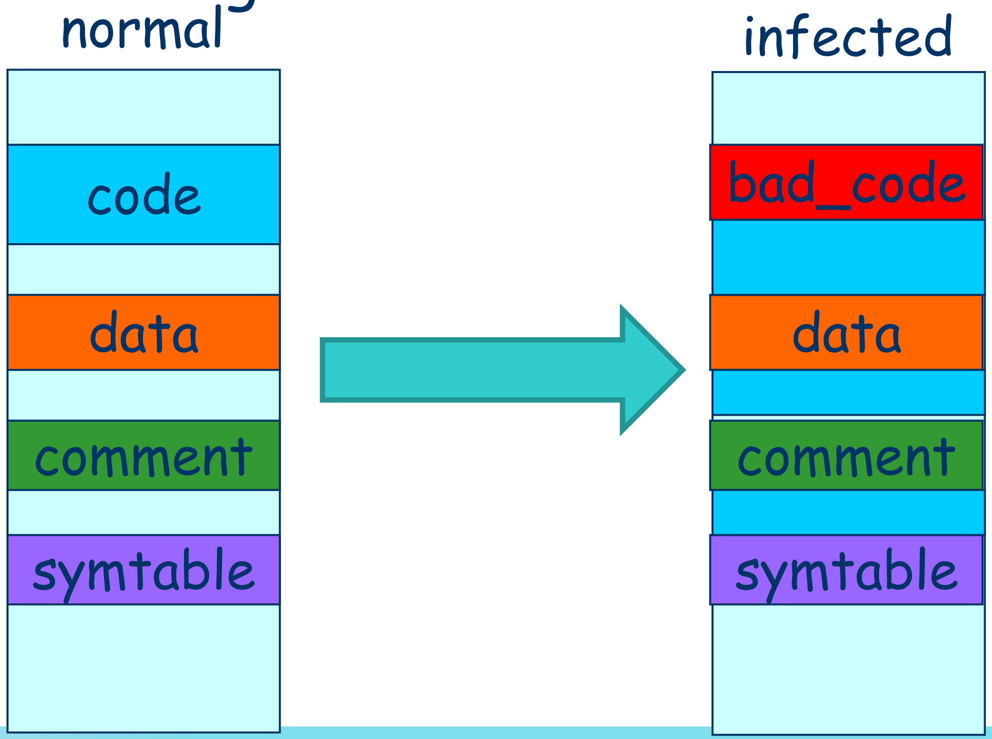
- 计算机一旦感染病毒应先断开网络（包括互联网和局域网），再进行杀毒，避免病毒在更大范围内传播，造成更严重的危害
- 由于邮件病毒的特征较为鲜明，对邮件的附件，不要随便运行
- 定期升级杀毒软件，启动“实时监控”和“个人防火墙”

林汉志 [illegible]

- created by 陳盈豪
- spread under the PE file format
  - only under Windows 95, 98, and ME
- overwrite the first 1024KB of the hard drive
  - hang, blue screen of death
- try to write to the Flash BIOS
  - the computer will not start at all

CIH - infection

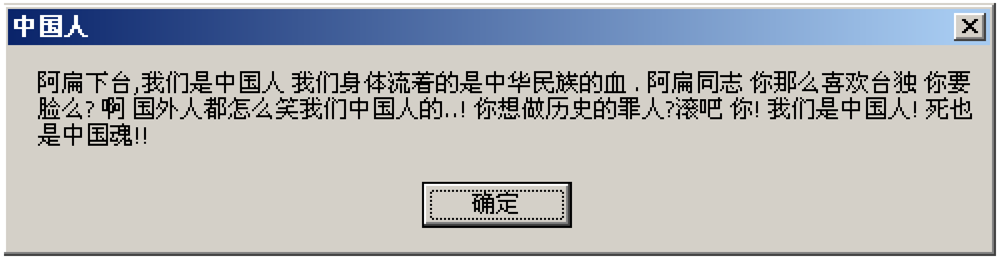
- “Spacefiller”
  - size does not grow



KillDPT (2009)

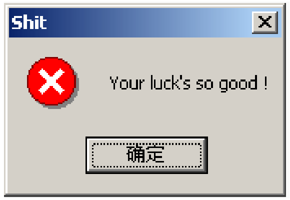
http://www.pusuo.net/2009-08-09/110305014.html

- attack machine with specific OS language
  - Big5



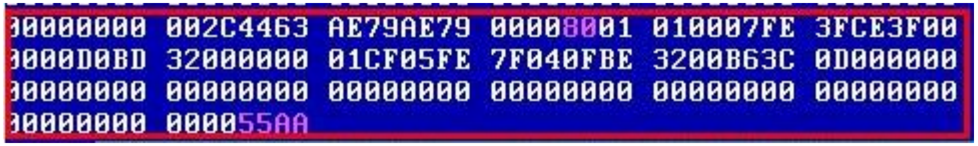
阿扁下台,我们是中国人 我们身体流着的是中华民族的血 . 阿扁同志 你那么喜欢台独 你要脸么? 啊 国外人都怎么笑我们中国人的..! 你想做历史的罪人?滚吧 你! 我们是中国人! 死也是中国魂!!

  - other

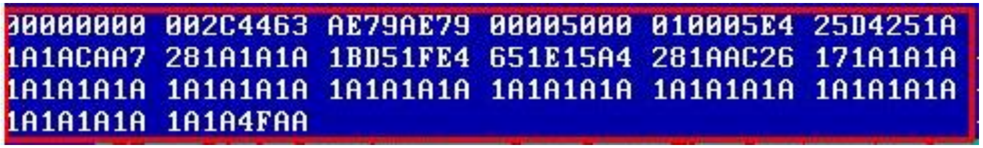


Your luck's so good !

  - Japanese



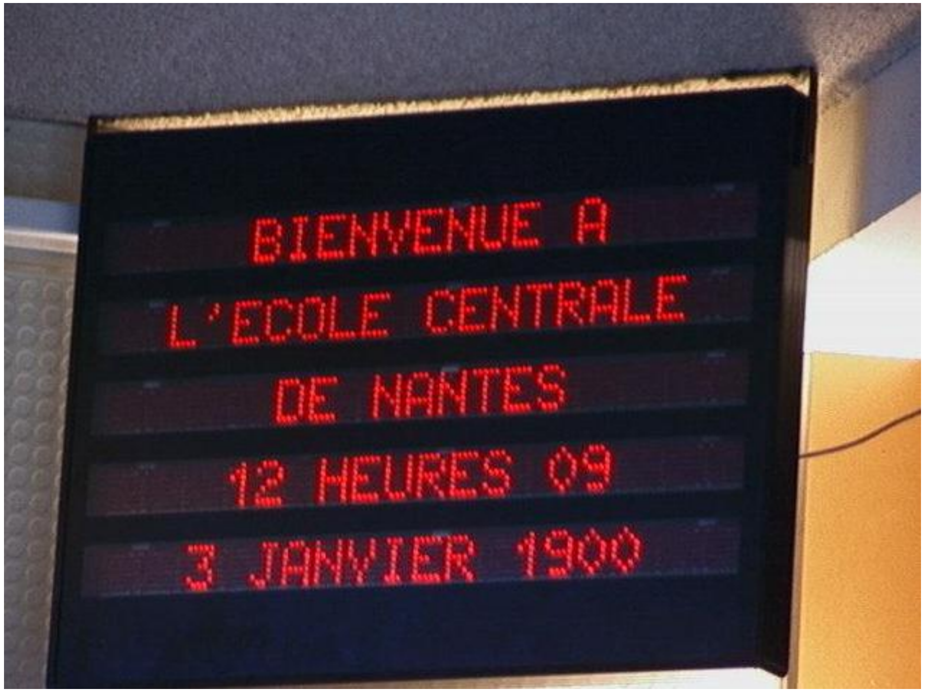
```
00000000 002C4463 AE79AE79 00008001 010007FE 3FCE3F00
0000D0BD 32000000 01CF05FE 7F040FBE 3200B63C 0D000000
00000000 00000000 00000000 00000000 00000000 00000000
00000000 000055AA
```



```
00000000 002C4463 AE79AE79 00005000 010005E4 25D4251A
1A1ACAA7 281A1A1A 1BD51FE4 651E15A4 281AAC26 171A1A1A
1A1A1A1A 1A1A1A1A 1A1A1A1A 1A1A1A1A 1A1A1A1A 1A1A1A1A
1A1A1A1A 1A1A4FAA
```

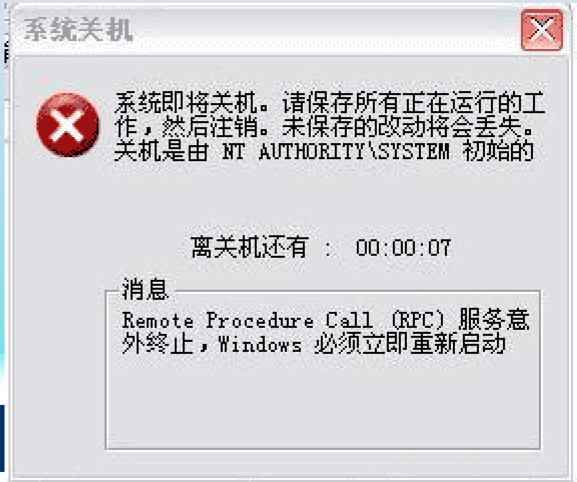
Y2K bugs (2000)

- BCD code
  - 0x99 + 1 = 0x00
- leap year



- 2010-bug
  - 用户收到的在2010年1月1日后发送的短信，都会显示为2016年1月1日。

Blaster (2003)



系统即将关机。请保存所有正在运行的工作，然后注销。未保存的改动将会丢失。关机是由 NT AUTHORITY\SYSTEM 初始的

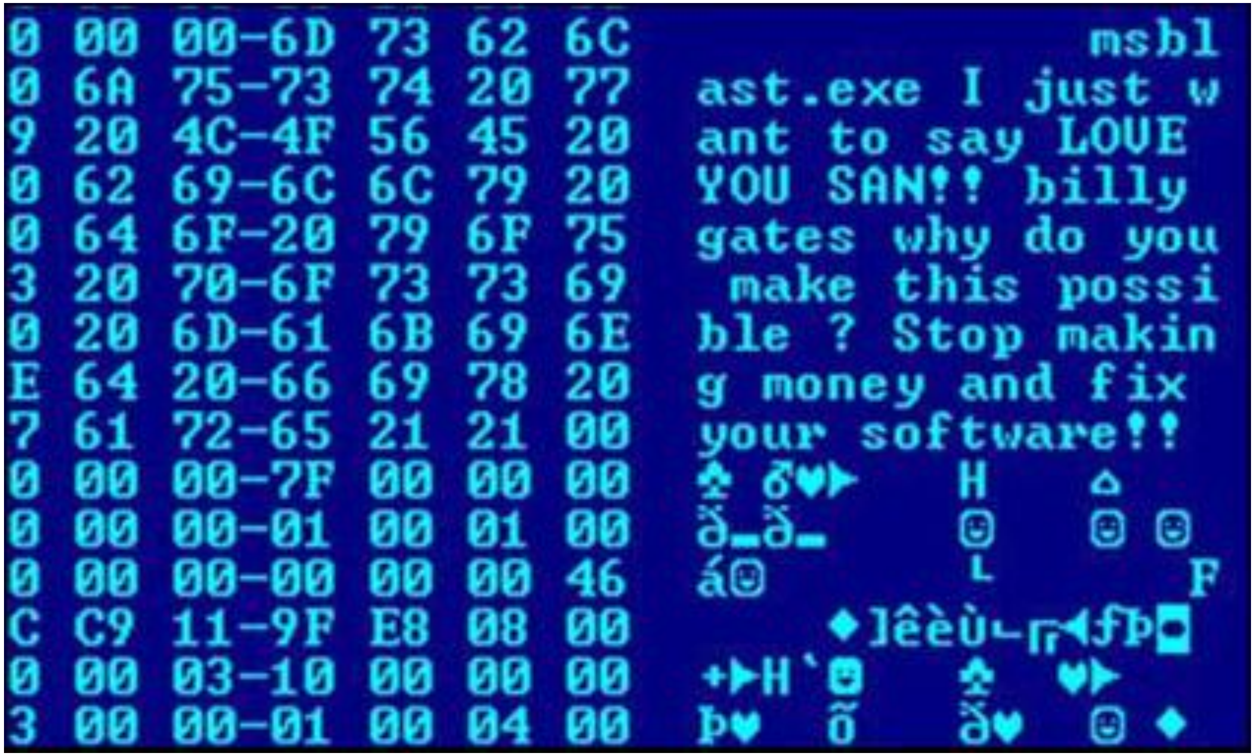
离关机还有 ： 00:00:07

消息

Remote Procedure Call (RPC) 服务意外终止，Windows 必须立即重新启动

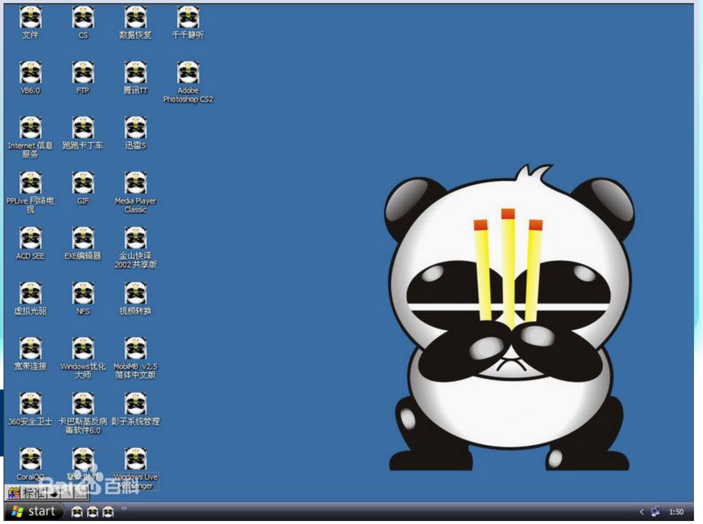
- spread by exploiting a buffer overflow in the DCOM RPC service
- start a SYN flood against windowsupdate.com
  - if the system date is after August 15 and before December 31st and after the 15th day of other months
  - create a distributed denial of service attack (DDoS)

Blaster - executable



```
0 00 00-6D 73 62 6C               msbl
0 6A 75-73 74 20 77   ast.exe I just w
9 20 4C-4F 56 45 20   ant to say LOVE
0 62 69-6C 6C 79 20   YOU SAN!! billy
0 64 6F-20 79 6F 75   gates why do you
3 20 70-6F 73 73 69    make this possi
0 20 6D-61 6B 69 6E   ble ? Stop makin
E 64 20-66 69 78 20   g money and fix
7 61 72-65 21 21 00   your software!!
0 00 00-7F 00 00 00   ♠ δ♥►    H   ⌂
0 00 00-01 00 01 00   ð▬ð▬     ☺   ☺ ☺
0 00 00-00 00 00 46   á☺       └      F
C C9 11-9F E8 08 00       ♦]êèù└╓◄ƒÞ▄
0 00 03-10 00 00 00    +►H`☻    ♠   ♥►
3 00 00-01 00 04 00   Þ♥   õ    ð♥  ☺ ♦
```

熊猫烧香 (2006)



- 每隔1秒
  - 寻找桌面窗口，并关闭窗口标题中含有以下字符的程序
    - 杀毒, 毒霸, 瑞星, 江民……
  - 并中止系统中以下的进程
    - VsTskMgr.exe, scan32.exe, CCenter.exe, KVXP.kxp……
- 每隔18秒点击病毒作者指定的网页
- 每隔10秒下载病毒作者指定的文件
- 每隔6秒
  - 删除安全软件在注册表中的键值
  - 修改以下值不显示隐藏文件
    - …\Advanced\Folder\Hidden\SHOWALLCheckedValue -> 0x00
  - 删除以下服务: ……
- ……

Do they have something to do with OS?

- Definitely!
- All of them are caused/propagated by bugs in OS.
- OS provides unnecessary rights ➔ insecurity
  - tradeoff between security and performance
- Attacking/Defending requires your wisdom of computer system!