2019 年信息安全工程师下午真题

试题一(共 14 分)

阅读下列说明，回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

【说明】

访问控制是保障信息系统安全的主要策略之一,其主要任务是保证系统资源不被非法使用和非常规访问。访问控制规定了主体对客体访向的限制，并在身份认证的碁础上，对用户提出的资源访问请求加以控制。当前,主要的访问控制模型包括：自主访问控制（DAC）模型和强制访问控制(MAC)模型。

【问题 1】(6 分)

针对信息系统的访问控制包含哪三个基本要素？

【问题 2】(4 分)

BLP 模型是一种强制访问控制模型，请问：

（1）BLP 模型保证了信息的机密性还是完整性？

（2）BLP 模型采用的访问控制策略是上读下写还是下读上写？

【问题 3】(4 分)

Linux 系统中可以通过 Is•命令查看文件的权限，例如：文件 net.txt 的权限属性如下所示：

```
-rwx-------1 root root 5025 May 25 2019 /home/abc/net.txt
```

请问：

（1）文件 net.txt 属于系统的哪个用户？

（2）文件 net.txt 权限的数字表示是什么？

试题二(共 13 分)

阅读下列说明和表，回答问题 1 至问题 3,将解答填入答题纸的对应栏内。

【说明】

密码学作为信息安全的关键技术，在信息安全领域有着广泛的应用。.密码学中，根据加密和解密过程所采用密钥的特点可以将密码算法分为两类：对称密码算法和非对称密码算法。此外，密码技术还用于信息鉴别、数据完整性检验、数字签名等。

【问题 1】(6 分)

信息安全的基本目标包括真实性、保密性、完整性、不可否认性、可控性、可用 性、可审查性等。密码学的三大安全百标 C.I.A 分别表示什么？

【问题 2】(5 分)

仿射密码是一种典型的对称密码算法。仿射密码体制的定义如下：

令明文和密文空间 M= C =Z_{26}，密钥空间 $K=\{(k_1,k_2)\in Z_{26}\times Z_{26}:\gcd(k_1,26)=1\}$。

对

任意的密钥 $key=(k_1,k_2)\in K,\ x\in M,\ y\in C,$ 定义加密和解密的过程如下：

$$\text{加密：}\ e_{key}(x)=(k_1x+k_2)\bmod 26$$

$$\text{解密：}\ d_{key}(y)=k_1^{-1}(y-k_2)\bmod 26$$

其中 k_1^{-1}表示 k_1在 Z_{26}中的乘法逆元，即 k_1^{-1}乘以 k_1对 26 取模等于 1，gcd(k_1, 26)= 1 表示 k_1与 26 互素。

设已知仿射密码的密钥 fey = (11，3)，英文字符和整数之间的对应关系如表 2.1。则：

表 2.1

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(1) 整数 11 在 Z_{26}中的乘法逆元是多少?

(2) 假设明文消息为“SEC”，相应的密文消息是什么?

【问题 3】(2 分)

根据表 2.1 的对应关系,仿射密码中,如果已知明文“E”对应密交“C″,明文“T”对应密文“F”,则相应的 key=(k_1, k_2)等于多少?

试题三（共 12 分）

阅读下列说明，回答问题 1 至问题 5,将解答填入答题纸的对应栏内。

【说明】

假设用户 A 和用户 B 为了互相验证对方的身份，设计了如下通信协议：

1. A→B:R_A
2. B→A:f(P_{AB}||R_A)
3. A→B: f(P_{AB}||___)

其中：R_A、R_B是随机数，P_{AB}是双方事先约定并共享的口令，“||”表示连接操作。f 是哈希函数。

【问题 1】（2 分）

身份认证可以通过用户知道什么、用户拥有什么和用户的生理特征等方法来验证。请问上述通信协议是采用哪种方法实现的?

【问题 2】（2 分）

根据身份的互相验证需求，补充协议第 3 步的空白内容。

【问题 3】（2 分）

通常哈希函数 f 需要满足下列性质：单向性、抗弱碰撞性、抗强碰撞性。.如果某哈希函数 f 具备：找到任何满足 f（x）=f（y）的偶对（x，y）在计算上是不可行的，请说明其满足哪条性质。

【问题 4】（2 分）
上述协议不能防止重放攻击，以下哪种改进方式能使其防止重放攻击？
（1）在发送消息加上时间参量。
（2）在发送消息加上随机数。
【问题 5】（4 分）
如果将哈希函数替换成对称加密函数，是否可以提高该协议的安全性？为什么？
试题四（共 19 分）
阅读下列说明和表，回答问题 1 至问题 4,将解答填入答题纸的对应栏内。
【说明】
防火墙类似于我国古代的护城河，可以阻挡敌人的进攻。在网络安全中，防火墙主要用于逻辑隔离外部网络与受保护的内部网络。防火墙通过使用各种安全规则来实现网络的 安全策略。
防火墙的安全规则由匹配条件和处理方式两个部分共同构成。网络流量通过防火墙时，根据数据包中的某些特定字段进行计算以后如果满足匹配条件，就必须采用规则中的处理方式进行处理。
【问题 1】（5 分）
假设某企业内部网（202.114.63.0/24）需要通过防火墙与外部网络互连，其防火墙的过滤规则实例如表 4.1 所示。

表 4.1

序号	源地址	源端口	目的地址	目的端口	协议	ACK	动作（处理方式）
A	202.114.63.0/24	>1024	*	80	TCP	*	accept
B	*	80	202.114.63.0/24	>1024	TCP	Yes	accept
C	*	>1024	202.114.64.125	80	TCP	*	accept
D	202.114.64.125	80	*	>1024	TCP	Yes	accept
E	202.114.63.0/24	>1024	*	（1）	UDP	*	accept
F	*	53	202.114.63.0/24	>1024	UDP	*	accept
G	*	*	*	*	*	*	（2）

表中“*”表示通配符，任意服务端口都有两条规则。
请补充表 4.1 中的内容（1）和（2），并根据上述规则表给出该企业对应的安全需求。【问题 2】（4 分）
一般来说，安全规则无法覆盖所有的网络流量。因此防火墙都有一条缺省（默认）规则，该规则能覆盖事先无法预料的网络流量。请问缺省规则的两种选择是什么？
【问题 3】（6 分）
请给出防火墙规则中的三种数据包处理方式。
【问题 4】（4 分）
防火墙的目的是实施访问控制和加强站点安全策略，其访问控制包含四个方面的内 容：服务控制、方向控制、用户控制和行为控制。请问表 4.1 中，规则 A 涉及访问控制的哪几个方面的内容？

试题五（共 17 分）
阅读下列说明和图，回答问题 1 至问题 4,将解答填入答题纸的对应栏内。
【说明】
信息系统安全开发生命周期（Security Development Life Cycle（SDLC））是微软提出的

从安全角度指导软件开发过程的管理模式，它将安全纳入信息系统开发生命周期的所有阶段，各阶段的安全措施与步骤如下图 5.1 所示。

图 5.1

【问题 1】（4 分）

在培训阶段，需要对员工进行安全意识培训，要求员工向弱口令说不！针对弱口令最有效的攻击方式是什么？以下口令中，密码强度最高的是（　）。

A. security2019

B. 2019Security

C. Security@2019

D. Security2019

【问题 2】（6 分）

在大数据时代,个人数据正被动地被企业搜集并利用。在需求分析阶段,需要考虑采用隐私保护技术防止隐私泄露。从数据挖掘的角度,隐私保护技术主要有:基于数据失真的隐私保护技术、基于数据加密的隐私保护技术、基于数据匿名隐私保护技术。

请问以下隐私保护技术分别属于上述三种隐私保护技术的哪一种?

（1）随机化过程修改敏感数据

（2）基于泛化的隐私保护技术

（3）安全多方计算隐私保护技术

【问题 3】（4 分）

有下述口令验证代码：

```
#define PASSWORD "1234567"
int verify_password (char *password)
{
   int authenticated;
   char buffer[8];
   authenticated=strcmp(password,PASSWORD);
   strcpy(buffer,password);
   return authenticated;
```

```
}
int main(int argc, char* argv[])
{
  int valid_flag=0;
  char password[1024];
  while(1)
  {
    printf("please input password: ");
    scanf("%s",password);
    valid_flag = verify_password(password); //验证口令
    if(valid_flag) //口令无效
    {
      printf("incorrect password!\n\n");
    }
    else   //口令有效
    {
      printf("Congratulation! You have passed the verification!\n");
      break;
    }
  }
```

其中 main 函数在调用 verify_password 函数进行口令验证时，堆栈的布局如图 5.2 所示。

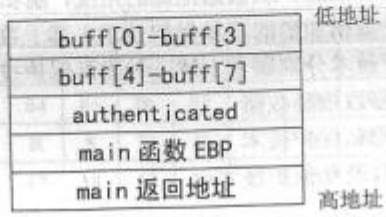

图 5.2

请问调用 verify_password 函数的参数满足什么条件，就可以在不知道真实口令的情况下绕过口令验证功能？

【问题 4】（3 分）

SDLC 安全开发模型的实现阶段给出了 3 种可以采取的安全措施，请结合问题 3 的代码举例说明？