第1讲 初始信息安全

1.1 测试点 1-1

（1）以下描述中体现了信息的何种特性
（A）书中自有黄金屋，书中自有颜如玉 价值性
（B）一传十，十传百 传递性
（C）没事别翻老黄历 时效性
（D）一个人不能两次踏入同一条河流 时效性
（E）古有飞鸽传书，今有网络通信 载体依附性
（F）兵者诡道也，实则虚之，虚则实之 真伪性
（G）世间万物皆有运行规律，掌握规律才能使人类与自然和谐共生 可处理性

1.2 测试点 1-2

（1）信息的安全属性在不同应用环境下的重要性（优先级）是不一样的，思考以下应用场景，给出你自己对系统中保密性、完整性和可用性的优先级判断并说明理由。
（A）学校的门户网站，包括院系介绍，教师社区，课程资源等服务内容；
（B）电力部门的输送电控制系统，包括电力终端设备状态监控、电力配送调度管理等服务内容；
（C）某研究所的科研成果管理系统，包括产品设计方案管理，实验测试参数管理等服务内容。
答：（A）中完整性>可用性>保密性，因为门户网站主要功能是发布信息，首先要保障信息的真实有效，不能被非授权修改，其实需要较高的可用性以方便访问，不存在涉密信息因此保密性要求最低；（B）中可用性>完整性>保密性，输送电控制系统为实时控制系统，因此具有高可用性要求，系统完整性是高可用性的必要保障，同时系统中不存储特殊的敏感信息；（C）中保密性>完整性>可用性，系统中数据具有敏感性，不能泄露，对数据的修改也需要在授权条件下，非实时控制系统相对而言可用性要求不高。

1.3 测试点 1-3

（1）场景一：用户 A 发送文件给用户 B。文件中包含需要保护的敏感信息，没有被授权阅读文件的用户 C 可以监听到文件发送的过程，并在文件传输过程中获得了一份文件的副本。

（2）场景二：网络管理员 D 发送包含用户授权信息的消息给计算机 E，计算机 E 接收后会自动更新本地的授权文件。用户 F 截取了消息，修改后发送给计算机 E，后者接收后认为来自于管理员 D，之后相应地更新了授权文件。

（A）问题一：上述场景中何种信息安全属性受到了破坏？

（B）问题二：上述场景中存在的安全威胁是什么？属于哪种威胁？

（C）问题三：实施的攻击行为属于哪种类型？

答：（1）中保密性受到破坏，（2）中完整性受到破坏；（1）信息泄露，（2）完整性破坏，均属于人为威胁；（1）属于被动攻击；（2）属于主动攻击。

1.4 测试点 1-4

（1）信息安全发展主要经历了哪些阶段，每一阶段的特征和标志性成果是什么？

（2）对信息安全有哪些基本认识？请举例进行说明。

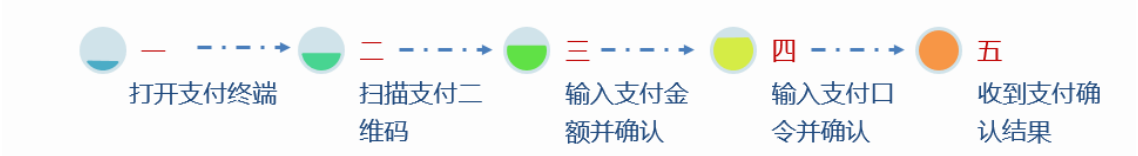
答：略，见课件。

1.5 测试点 1-5

（1）数据安全与内容安全有什么区别？

（2）举例说明安全服务与安全机制的关系。

（3）移动支付是目前应用最广泛的网络服务之一，以下为消费者在支付过程中的各个环节，请分析在各环节中移动支付系统必须提供的安全服务。请分析在各环节中移动支付系统必须提供的安全服务。



（1）答：略，参见课件。

（2）答：安全服务是指系统提供的安全防护措施，安全机制用来实施安全服务的机制，服务是需求，机制是手段，安全服务和安全机制是多对多的关系，例如密

码技术是一种可以实现数据机密性又能实现数据完整性的机制，反之数据机密性除了用密码技术也可使用业务流填充，路由控制等机制来实现。

（3）答：打开支付终端需要提供身份鉴别服务，扫描二维码需要提供访问控制服务（授权使用摄像头），输入金额并确认需要提供数据完整性服务，输入口令并支付需要提供数据机密性服务，收到确认结果需要提供不可否认性服务。

1.6 测试点 1-7

（1）结合“棱镜门事件”，谈谈对“没有网络安全就没有国家安全”的理解。

（2）思考：一名合格的信息安全人才应该具备什么样的素质？

（1）答：网络安全上升到国家战略高度，与政治、经济、社会、文化、军事安全密切相关。棱镜门事件是利用网络霸权，威胁国家安全的典型案例。外部威胁和内部的脆弱性并存，因此国家安全与网络安全存在密切关联。（重要性+风险分析=安全形势）

（2）答：政治强、业务精、作风好（坚定的政治立场，过硬的职业技能，优秀的职业道德，严谨的工作作风）。

第2讲 信息安全技术概述

2.1 测试点 2-1

（1）密码学是什么？其研究工作分为哪两个方向？

（2）密码学发展经历了那几个阶段？每个阶段的特点是什么？

（3）依据密码体制的定义，给出对凯撒密码体制的明文空间、密文空间、加密方法、解密方法、密钥空间的描述。

（4）对称加密和公钥加密在密钥使用上存在差异，试考虑这样的场景：如果有一个单位有 N 名员工，员工间的网络通信需要保密，采用对称加密需要分配多少个密钥？采用公钥加密需要多少个密钥？

（5）依据凯撒密码体制的工作原理，编制一个可以实现对英文语句进行加解密转换的 C 语言程序。

（1）答：略，参见课件。

（2）答：略，参见课件。

（3）答：略，参见课件。

（4）答：对称加密需要C_n^2个，公钥加密需要n对密钥。

（5）参考代码：

```
/*凯撒加密算法实现*/
#include <stdio.h>
#include <string.h>

int main()
{
    char passwd[100], encrypted[100];
    int i, j, k, t, move;
    while(1)
    {
        printf("Enter message to be encrypted:");
```

```
        gets(passwd);
        printf("Enter shift amount(1-25):");
        scanf("%d%*c",&move);
        for(i=0; i<strlen(passwd); i++)
        {
            if(passwd[i] >= 'A' && passwd[i] <= 'Z')
            {
                passwd[i] = ((passwd[i]-'A')+move)%26+'A';
            }
            else if(passwd[i] >= 'a' && passwd[i] <= 'z')
            {
                passwd[i] = ((passwd[i]-'a')+move)%26+'a';
            }
        }
        printf("%s",passwd);
        printf("\n");
    }
    return 0;
}
```

2.2 测试点 2-2

（1）物理安全包括那些方面？解决物理安全的技术途径有哪些？

（2）手机是当前社会环境下重要的个人信息设备，为保护手机的物理安全，谈谈你是如何做的？

（3）某单位对机房环境有严格的安全要求，在机房墙体内设置了金属网，请问该措施的目的是什么？除了该措施，还有哪些措施可以用于同样的目的？

（4）提高系统可靠性的技术手段主要包括哪些？灾备系统往往被称为异地灾备系统，为什么要强调“异地”？

（5）使用分布式系统的主要目的是什么？在分布式系统中通常将任务进行分解，由统一的任务调度和负载均衡机制将子任务分配到不同的主机上执行，如果一套

分布式系统包括 N 台主机，需要至少 T 台主机正常工作才能保证任务的基本执行，每台主机的出现故障的概率为 p，试问该分布式系统正常工作的概率 P 是多少？

（1）答：略，参见课件。

（2）答：提示物理安全包括实体、环境和管理安全，手机有没有对本身的保护措施，防摔、防盗、防水等？对使用环境有没有注意，高湿、高腐蚀环境等？管理上有没有随意放置等行为？

（3）答：电磁屏蔽，此外还有电磁抑制和电磁干扰手段。

（4）答：避错、纠错、容错和容灾。异地主要是最大限度提高系统的可靠性，在空间上规避灾难带了的风险。

（5）答：$\sum_{i=T}^{N} C_N^i * (1-p)^i * p^{n-i}$

2.3 测试点 2-3

（1）常见的身份认证方法有哪几种？分别列举出你具体使用过认证方法实例？

（2）身份认证技术是如何划分的？手机网银支付的认证属于哪一类认证技术，需要提供哪些认证凭据？

（3）有人说“刷脸认证”是最安全的认证方式，你认为这种说法是否正确？为什么？（提示：可以“图像对抗攻击”为关键词进行查询）

（1）答：略，参见课件。

（2）答：略，参见课件；多因子动态认证，手机网银登录口令、支付口令和验证码。

（3）答：不正确，第一生物特征认证同样存在泄露风险，且泄露后很难修改。目前，对刷脸等生物特征认证也有针对性的攻击手段，如通过图像对抗攻击绕过认证过程。

2.4 测试点 2-4

（1）ACL 和 ACCL 各自有什么优缺点？请举例进行说明。

（2）系统中有三个用户 Usr1，Usr2 和 Usr3， Usr1 创建了日志文件 File1，允许 Usr2 向文件中写入操作记录，允许 Usr3 打开文件查看 Usr2 的操作记录；Usr2 创建了一个通信进程，该通信进程允许 Usr1 收发消息，但只允许 Usr3 接收消息；Usr3 创建了一个共享存储区，允许 Usr1 读存储区内容，Usr2 读写存储区内容。根据上述描述，画出对应的 ACL 和 ACCL。

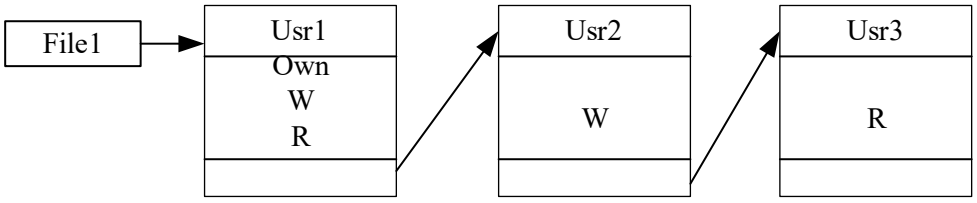
（3）能否使用 ACL 或 ACCL 机制来实现基于角色的访问控制？如果不能，你能否给出实现 RBAC 的技术思路？

（4）在 Windows 操作系统中建立一个文件，并对文件的访问权限进行管理，判断 Windows 操作系统采用的访问控制模型，说明自己的判断理由。

（1）答：略，参见课件。

（2）答：ACL 是以客体为中心建立的访问控制列表，ACCL 是以主体为中心建立的访问控制列表，具体如下。

ACL：



Proc1 和 Buf1 的 ACL（略）

ACCL：略。

（3）不能够直接使用 ACL 或 ACCL 来实现 RBAC，因为在 RBAC 中采用了角色作为权限分配的桥梁，需要在 ACL 或 ACCL 的基础上增加用于建立角色—权限许可，主体—角色关联的数据结构。主要包括：用户表、角色表、权限表、角色权限表和用户角色表。

（4）自主访问控制，因为权限直接和用户关联，且可以有创建者（拥有者）管理。

第3讲 信息安全的攻与防

3.1 测试点 3-1

（1）假设你在网站上观看视频时，你看到一个弹出窗口要求你安装定制的解码器，才能正常观看视频。如果同意安装，你的计算机有可能会面临什么威胁？

（2）以表格方式对比传统型病毒、蠕虫和木马的特点，指出各自专属的特征。

（1）答：有可能被植入恶意代码，对计算机系统的保密性、完整性和可用性都可能造成破坏，信息泄露、信息伪造、完整性破坏等威胁都会存在。（可举例说明）

（2）答：

恶意代码类型	主要特征	破坏行为	专属特征
传统型病毒	寄生性、传染性、潜伏性、触发性和破坏性	良性（干扰计算机执行）、恶性（破坏文件系统，删除数据……）	寄生性
蠕虫	自传播性、隐蔽性、破坏性	拥塞网络、破坏系统	自传播性
木马	隐蔽性、非授权性/远程控制	信息窃取、远程控制	远程控制

3.2 测试点 3-2

（1）通过查阅资料，进一步对 APT 攻击进行了解，并以一种 APT 攻击的流程为例，对 APT 攻击的特点进行阐述。

（2）Ping 是系统提供的用于检测网络连通性的程序，有人认为这样的程序不会对计算机系统的安全造成损害，因此没有危害性，谈谈你自己的观点，并加以说明。

（1）答：例如韩国平昌冬奥会 APT 攻击，流程（略）。特点：攻击特征难以提取；攻击行为隐蔽性强；攻击渠道复杂；攻击手段多样；攻击时间持续。

（2）答：观点错误，Ping 可以用于网络探测，因此也存在使用上的风险。

3.3 测试点 3-3

（1）防火墙和网闸都能提供在网络边界上的安全防护作用，请分析两者在功能上的相同与不同之处。

（2）漏报率和误报率是入侵检测系统（IDS）重要的性能指标，有人认为采用异常检测技术的 IDS 误报率很高，没有实用价值，请给出你的判断并说明判断理由。

（1）答：都是隔离技术，网闸属于物理隔离，防火墙属于逻辑隔离，实现原理和功能都要显著区别。具体如下：（略）

（2）答：观点错误，异常检测能检测到未知入侵，因此有重要的应用价值。

第4讲 信息安全管理概述

4.1 测试点 4-1

（1）什么是信息安全管理中的 PDCA 模型？
（2）我国的信息安全法律法规体系是如何构成的？
（3）有人说西方的网络环境是开放自由的，公民在网络空间中的行为不会受到管理和监控，这种观点是正确的吗？请查阅相关资料，谈谈自己的看法。
（1）答：略，参见课件。
（2）答：略，参见课件。
（3）答：错误，例如美国的《爱国者法案》规定了政府可以行使严格的管理和监控权，对网络空间进行监管是各国的惯例。

4.2 测试点 4-2

（1）请查阅《中华人民共和国网络安全法》，回答以下问题：
（A）网络安全法是如何规范个人信息收集行为的？
（B）网络安全法是如何斩断信息买卖利益链的？
（C）网络安全法是如何防范个人信息泄露的？
（D）网络安全法是如何对网络诈骗溯源追责？
答：略，参见课件。

4.3 测试点 4-3

（1）GB17895-1999《计算机信息系统安全保护等级划分准则》中划分了哪几种安全等级？
（2）GB/T 22239-2019 《网络安全等级保护基本要求》中分别对哪几类信息系统做出了专门规定？
（3）概述等级保护的工作流程。
（4）假定有一个由银行提供代水电代收费服务的信息系统，如果该系统受到破坏，将导致个人或企业无法通过银行网点缴纳相关费用，水电公司的收费业务只能在

其处理能力有限营业厅进行，导致业务能力大幅度下降，依据等级保护的定级规则，思考该系统应属于几级保护的对象？

（1）答：略，参见课件。

（2）答：略，参见课件。

（3）答：略，参见课件。

（4）答：依据受侵害客体和侵害程度进行判断，客体为水电公司为企业法人，收费业务能力大幅下降没有丧失，属于严重损害，综合上述分析，系统属于网络安全二级保护对象。

4.4 测试点 4-4

（1）作为一名从事信息安全专业的人员，应该如何从自身做起，共同营造清朗的网络环境？

答：提示（两个方面，底线是遵纪守法，要求是严守网络行为道德规范）。