**第一章习题参考答案**

**1.信息系统和信息系统安全的定义？**

**参考答案：**信息系统是指信息产生、存储、处理、传输和使用的人-机一体化计算机系统，包括：计算机硬件、软件、固件、网络和人员。

信息系统安全是指保证信息系统的硬件、软件或固件、网络不因偶然的或恶意的原因而遭受破坏、更改、访问和泄露，从而保证信息系统能够连续可靠地正常运行，提供稳定的服务。

**2.如果信息系统无任何脆弱性，是否就不存在安全问题呢？分析举例**。

**要点：**（1）系统的安全问题根源；（2）脆弱性是系统存在安全问题的充分条件而非必要条件；（3）举例说明。

**参考答案：**信息系统安全问题的来源包括信息系统自身的开放性、脆弱性，以及对于系统的人为恶意入侵。即使信息系统无任何脆弱性，也会受到来自包括自然因素和人为因素的安全威胁，从而带来安全问题。例如，对信息系统的人为电磁干扰，属于人为进行的物理攻击，通过物理接触信息系统以及其周边设备，对信息系统的软硬件和数据进行破坏。

**3.如何理解信息系统的开放性？举一个书本以外的例子。**

**要点：**（1）什么是开放性；（2）开放性的优缺点；（3）举例

**参考答案：**信息系统的开放性是指除了系统的私有信息（如：登录密码）外，其硬件和软件都是对外公开的，其设计标准、采用的接口都是依据公开标准，任何用户、网络和应用都可以免费接入系统

开放性的优点是：（1）采用标准的设备或协议；（2）能兼容不同厂家的产品；……

开放性的缺点是：（1）系统的缺陷容易被捕获和利用；（2）安全性低；……

例如USB(通用串行总线标准)，是一个外部总线标准，用于规范电脑与外部设备的连接和通讯。是应用在PC领域的接口技术。

**4.信息系统的安全风险和安全威胁分别体现在哪些方面？简要阐述**。

要点：（1）安全风险包含的6个方面内容；（2）安全威胁包含的4个发面内容；（3）分别简要阐述。

参考答案：安全风险主要包括：（1）电磁泄漏；（2）芯片的脆弱性；（3）操作系统漏洞；（4）数据库漏洞；（5）通信协议漏洞；（6）移动存储介质安全漏洞。

安全威胁主要来源于自然因素和人为因素，主要体现在：（1）物理攻击；（2）网络攻击；（3）恶意代码入侵；（4）安全管理。

分别阐述上述内容：（略）

**5.信息系统的基本安全属性包含哪些？除此之外，你认为信息系统还需要有哪些安**

**全需求？举例说明。**

**要点：**（1）安全属性（保密性、完整性和可用性）；（2）至少说2个方面的安全需求，并简要阐述。

**参考答案：**基本安全属性包括：保密性、完整性、可用性。

信息系统还需具备漏洞监测与系统安全风险评估机制。识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解信息系统本身的脆弱性，评估所有存在的安全风险。例子：在主干网或者服务器中建设实时监测ddos流量攻击的机制，或者评估系统承载非法访问业务的能力。

**6.信息系统安全包含哪四个层面？其内涵是什么？分析它们之间的相互关系。**

**要点：**（1）系统安全包含的四个层面分别是什么；（2）每个层面的含义是什么；（3）它们之间的相互关系。

**参考答案：**针对信息系统，安全可以划分为以下四个层次：设备安全、数据安全、内容安全、行为安全。其中数据安全即是传统的信息安全。

1)设备安全

信息系统设备的安全是信息系统安全的首要问题。这里主要包括三个方面：

(1)设备的稳定性：设备在一定时间内不出故障的概率。

(2)设备的可靠性：设备能在一定时间内正常执行任务的概率。

(3)设备的可用性：设备随时可以正常使用的概率。

信息系统的设备安全是信息系统安全的物质基础。除了硬件设备外，软件系统也是一种设备，也要确保软件设备的安全。

2)数据安全

信息系统的安全属性包括保密性、完整性和可用性。很多情况下，即使信息系统设备没有受到损坏，但其数据安全也可能已经受到危害，如数据泄露、数据篡改等。由于危害数据安全的行为具有较高的隐蔽性，数据应用用户往往并不知情，因此，危害性很高。

3)内容安全

内容安全是信息安全在政治、法律、道德层次上的要求。

(1)信息内容在政治上是健康的。

(2)信息内容符合国家的法律法规。

(3)信息内容符合中华民族优良的道德规范。

除此之外，广义的内容安全还包括信息内容保密、知识产权保护、信息隐藏和隐私保护等诸多方面。

如果数据中充斥着不健康的、违法的、违背道德的内容，即使它是保密的、未被篡改的，也不能说是安全的。因为这会危害国家安全、危害社会稳定、危害精神文明。因此，必须在确保信息系统设备安全和数据安全的基础上，进一步确保信息内容的安全。

4)行为安全

数据安全本质上是一种静态的安全，而行为安全是一种动态安全。

(1)行为的秘密性：行为的过程和结果不能危害数据的秘密性。必要时，行为的过程和结果也应是秘密的。

(2)行为的完整性：行为的过程和结果不能危害数据的完整性，行为的过程和结果是预期的。

(3)行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正。

行为安全强调的是过程安全，体现在组成信息系统的硬件设备、软件设备和应用系统协调工作的程序（执行序列）符合系统设计的预期，这样才能保证信息系统的“安全可控”。

**7. 信息系统的开放性是信息系统安全问题的根源之一，本书中列举了 TCP 协议存在的安全漏洞。再举两个例子说明系统的开放性所带来的风险。**

**参考答案：**（1）本章第3题参考答案中的USB协议。日常使用的鼠标键盘都是基于UID协议的USB设备。在HID协议下，U盘的固件可以被黑客修改，植入恶意代码，将U盘伪装成键盘、网卡，进而操纵电脑、篡改DNS，完成下一步的攻击。除了U盘，其他USB设备同样可以伪装，例如利用充电宝盗取数据也屡见不鲜。

（2）关系型数据库系统通常使用一定规范的结构化查询语句（SQL）以进行数据查询，这导致在数据库系统内部的查询手段对外是开放的。以某些利用到数据库系统的商用web应用为例，这些应用在开发时可能会留有漏洞，使得攻击者恶意注入的SQL查询语句在未经授权的情况下被错误地执行，带来安全风险。