中原工学院信息商务学院

实 验 报 告

实验项目名称 《信息系统安全导论》课后习题

所属课程名称 信息系统安全导论

实 验 类 型 上机实验

实 验 日 期 2012/10/26

学 历 班 级 信管 104

学 号 201004034432

姓 名 张扬程

指 导 老 师 罗刘敏

第一章 习题与思考题

1．什么是信息系统？说明其发展经历的四个阶段。

答：信息系统是与信息加工，信息传递，信息存贮以及信息利用等有关的系统。其

发展经历了电子数据处理系统、管理信息系统、决策支持系统、办公自动化系统这四个阶段。

2．说明信息安全的内涵。

答：信息安全，概括的说，信息安全包括信息系统的安全和信息安全，并以信息安全为最终目标，信息安全又通过保密性、完整性、可用性和可控性的参数加以表征。具体指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。

3．分析网络和通信协议的脆弱性和缺陷。

答：缺乏对用户身份的鉴定、缺乏对路由协议的鉴别认证、TCP/UDP 的缺陷

4．威胁信息系统的主要方法有哪些？

答：比较常见的方法：冒充、旁路控制、破坏信息的完整性、重放、截收和辐射侦测、陷门、特洛伊木马、抵赖等。

5．说明信息系统安全的防御策略。

答：信息系统安全的防御策略主要包括以下：

①信息系统防御策略的基本原则：最小特权原则、纵深防御、建立控制点、监测和消除薄弱连接、失效保护原则、普遍参与、防御多样化、简单化原则

②信息系统安全的工程原则：系统性、相关性、动态性、相关性。

③典型信息系统的安全需求分析：景荣信息系统的安全需求、电子商务系统的安全需求、政务信息系统的安全需求、个人上网的安全需求

6．说明金融信息系统的安全需求原则。

答：授权原则、确认原则、跟踪原则、效能投资相容原则。

7．网络设备有哪些不安全因素？

答：网络设备容易遭受地震，水灾、火灾、有害气体和其他环境事故的破坏，同时在遭受迫害后资源的恢复过程难以有效保证。

8．如何从工作人员和环境条件方面提高信息系统的安全性？

答：①工作人员方面：设置信息系统的管理者，主要包括系统安全员、系统管理员、信息安全管理员、网络管理员、存储介质保管员、操作人员、软件维修人员

②境条件方面：电力供应、灾难应急、硬件设施、软件设施

9．什么是可信计算基（TCB）？

答：TCB 是一种实现安全策略的机制，包括硬件、固件和软件。它们根据安全策略来处理主题（系统管理员、安全管理员、用户、进程）对客体（进程、文件、纪录、设备等）的访问，TCB 还具有抗篡改的性质和易于分析与测试的结构。

10．详细说明安全标记保护级的可信计算基的功能。

答：⑴本级的计算机来看：可信计算基控制主体和客体，仅当满足一定条件时，主

题才能读/写一个客体。另外，可信计算基应维护与每个主体及其控制下的存储对象相关的敏感标记，敏感标记应准确地表示相关主体或客体的安全级别。
⑵在用户角度来看：①确定用户的访问权与授权数据。
②接受数据的安全级别，维护与每个主体及其控制下的存储对象相关的敏感标记。
③维护标记的完整性。
④维护审计标记信息的输出，并与相关的信息进行匹配。
⑤确保以该用户的名义而创建的那些在可信计算基外部的主体和授权，受其访问权限和授权的控制。

11．结构化保护级的主要特征有哪些？
答：①可信计算基基于基于一个明确定义的形式安全保护策略。
②将第三极实施的（自主和强制）访问控制扩展到所有主体和客体。
③针对隐蔽信道，将可信可信计算基构成为关键保护元素和非关键保护元素。
④可信计算基具有合理的接口，使其能经受严格测试和复查。
⑤通过提供可信路径来增强鉴别机制。
⑥支持系统管理员和操作员的可确认性，提供可信实施管理，增强严格的配置管理控制。

第二章 习题与思考题

1．解释国家标准 GB/T 18794-2003 的三维示意图（图 2.1）的意义。
答：①提供安全体系结构所匹配的安全服务和有关安全机制在体系结构下的一般描述
②确保体系结构内部可以提供相关安全服务的位置
③保证完整准确地配置安全服务，并且一直维持信息系统安全的生命期中，安全功能必须满足一定的强度的需求
④一种安全服务可以通过某种单独的安全机制提供，也可以通过多种安全机制联合提供

2.ISO 开放系统互连安全体系中设置了哪些服务功能？这些功能在 OSI 安全体系中处于什么位置？
答：⑴鉴别服务：提供对通信中对等实体和数据来源的鉴别，是最基本的安全服务之一。
⑵访问控制服务：对资源提供保护，以对抗其非授权使用和操纵，是安全服务的重要组成部分。
⑶机密性服务：保护信息不被泄露或暴露给未授权的实体，这种服务对数据提供保护使之不被非法授权泄露
⑷完整性服务：对数据提供保护，以对抗未授权的改变、删除或替代
⑸抗抵赖性服务：防止参与与某次通信交换的任何一方事后否认本次通信或通信的内容

3．说明 ISO 开放系统互连安全体系的安全机制。
答：〈1〉加密机制：是各种安全服务和其他许多安全机制的基础，既能为数据提供机密性，也能为通信业务流信息提供机密性，并且还能成为其他安全服务和安全机

制的一部分，其支持或补充作用。
〈2〉数字签名：是数据封装的一种特殊情况，它是对附加数据或数据单元的密码变换的结果，主要用于证实消息的真实来源，也是解决一个消息的发送者和接收者之间的争端的基础。
〈3〉访问控制机制：主要是用来对资源访问或操作加以限制的策略，主要是把对资源的访问只限于那些被授权的用户。
〈4〉完整性机制：目的是保护数据，以避免未经授权的数据乱序、丢失、重放，插入和篡改。
〈5〉鉴别交换机制：
①可用于鉴别交换的一些技术：使用鉴别信息、密码技术、使用该实物的特征或占有物。
②鉴别机制可设置在以提供对等实体鉴别。
③当采用密码技术时，这些技术可以与“握手”协议结合起来以防止重放（即确保存活期）
④鉴别交换技术的选用取决于使用他们的环境。在许多场合，他们必须与下列几项结合使用：时间标记与同步时钟、两方握手和三方握手、有数字签名和公正机制的抵赖服务。
〈6〉通信业务填充机制：提供业务流机密性的一个基本机制。包括生成伪造的通信实例、伪造的数据单元或伪造的数据单元中的数据。
〈7〉路由选择控制机制：路由能被动态地或预定的选取，以便只用物理上安全的子网络、中继站或链路来进行通信，保证敏感数据只在具有适当保护级别的路由器上传输。
〈8〉公正机制：有关在两个或多个实体之间通信的数据的性质，他的完整性、数据源、时间和目的地等，能借助公正机制得到保证。这种保证是由第三方公正人提供。公正认为通信实体所信任，并掌握必要信息以一种可证实方式提供所需的保证。每个通信事例可使用数字签名、加密和完整性机制以适应公正认提供的服务。

4．访问控制机制可以建立在哪些手段之上？
答：①访问控制信息库　②鉴别信息　③权利　④安全标记
⑤试图访问的时间　⑥试图访问的路由　⑦访问持续期

5．描述 OSI 安全服务和安全机制之间的关系。
答：1 对于每一种安全服务可以由一种机制单独提供，也可由几种机制联合提供,OSI 所能提供的 5 大类安全服务与 8 种安全机制的对应关系如表。

表 2-5　OSI 安全服务与安全机制之间的关系

安全服务	安全机制							
	加密	数字签名	访问控制	数据完整性	认证交换	通信业务填充	路由控制	公证
对等实体认证	Y	Y	-	-	Y	-	-	-
数据源认证	Y	Y	-	-	-	-	-	-
访问控制服务	-	-	Y	-	-	-	-	-
连接保密性	Y	-	-	-	-	-	Y	-
无连接保密性	Y	-	-	-	-	-	Y	-
选择字段保密性	Y		-	-	-			-
通信业务流保密性	Y	-	-	-	-	Y	Y	-
带恢复的连接完整性	Y	-	-	Y	-	-	-	-
不带恢复的连接完整性	Y	-	-	Y	-	-	-	-
选择字段的连接完整性	Y	-	-	Y	-	-	-	-
无连接完整性	Y	Y	-	Y	-	-	-	-
选择字段的无连接完整性	Y	Y	-	Y	-	-	-	-
有数据原发证明的抗否认	-	Y	-	Y	-	-	-	Y
交付证明的抗否认	-	Y	-	Y	-	-	-	Y

注：Y 为提供、－为不提供。

6．阐述 TCP/IP 协议模型中提供的安全服务类型。

答：网络接口层、网络层、传输层、应用层这四个层次的安全服务类型，具体的安全服务有：对等实体鉴别、数据源发鉴别、访问控制服务、链接机密性、无连接机密性、选择字段机密性、流量保密性、具有恢复能力的连接完整性、没有恢复能力的连接完整性。

7．OSI 的基本管理框架定义了哪些安全管理活动？

答：系统安全管理、安全服务管安全机制管理。

8．阐述信息系统安全管理重要意义和安全管理的主要内容。

答：〈1〉信息系统安全管理重要意义：有效的保护信息系统的安全，最大限度的减少面临的安全危险。

〈2〉安全管理的主要内容：①关于 OSI 安全服务的管理与安全机制的管理，要求给这些服务与机制分配管理信息，并收集于这些服务和机制的操作有关的信息，不强调在调用特定安全服务的协议中传递与安全有关的信息。

②安全信息库是一个概念的集存地，存储开放系统所需的安全有关的全部信息。

③管理协议特别是安全管理协议，以及传送这些管理信息的通信通道，潜在着抗攻击的脆弱性。

④安全管理可以要求在不同系统的行政管理机构之间交换与安全有关的信息，以便使 SMIB 得以建立扩展。

9．　举例说明实现 AH,ESP 的传输模式、隧道模式的工作模型。

AH 有两种工作方式：传输方式和隧道方式

10．　说明 TLS 协议包括那些步走？并用图示说明 TLS 握手流程。

11.TLS 握手协议包括哪些步骤？并用图示说明 TLS 握手流程。

12. TLS 协议有哪些基本消息。各有何作用？

Hello 消息服务器和客户端使用 hello 消息来交换与安全相关的信息,如随机数、ciphersuite；Sever Certificate 消息该消息表示服务器发送证书；Sever Key Request 消息服务器发送该消息只是客户提供其证书；Sever Hello Done 消息服务器发送该消息指示 Hello 阶段结束；Cilent Certificate 消息这是客户端接收到 Sever Hello Done 消息之后能够发送的第一条消息，该消息只有在服务器要求证书的情况下才能发送。如果客户没有合适的证书也可以发送不包含证书的 Cilent Certificate 消息；Client Key Exchange 消息该消息有客户端发送；Certificate Verify 消息该消息用来提供显示的客户证书校验；Finished 消息该消息在 Chang Cipher Spec 消息之后发送，用来校验密钥交换和鉴别工程是否成功。

13. OSI 的基本管理框架定义了那些安全管理活动？

系统安全管理；安全服务管理；安全机制管理：密钥管理、加密管理、数字签名管理、访问控制管理、完整性管理、鉴别管理、通信业务填充管理、路由选择控制管理、公证管理

14. 阐述信息系统安全管理的重要意义和安全管理的主要内容。