**安全体系结构**

1.（2014）一个典型的企业Internet网，内部用户通过统一认证平台访问内部各业务系统，内部终端既有通过RJ45网线连接的工作站，也有通过wifi连接的ipad，均对外共享一个x网公共IP地址出口通过NAT、应用代理服务器和一个IP过滤型防火墙接入互联网。试用IATF“三保卫一支撑”分解其深度保护区域并用简单网络拓扑图标注，对应“边界和接入”区域列出其对应的基本信息资产。（20分）

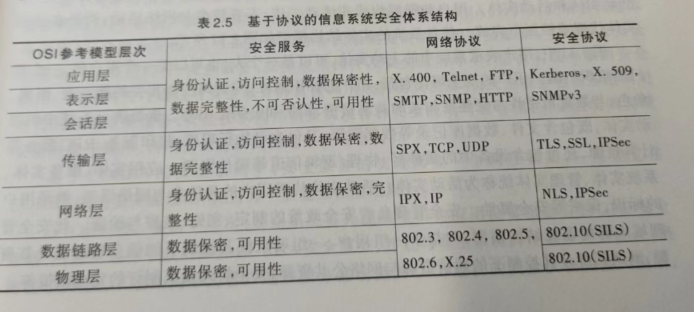
2.（2014）对应一个公共Ipv4广域网，分析保密性C在osi7层各层实施的可行性，分别对应七层明确给出：

（1）结论

（2）对不可实现的层，给出理由

（3）对可行的层，给出可能的实现方法（15分）

P56《信息安全体系结构》





3.（2014）基本的安全机制有哪些？当面临可能的身份冒用威胁时，分析在应用层抗重放攻击可以采取的安全机制。（15分）

P19+？

4.（2014）分析强制访问控制与自主访问控制之间的主要异同。（15分）

P73

|  |
| --- |
| **控制策略的设置者**  **自主访问控制：由客体的属主对自己的客体进行管理，由属主自己决定是否将自己的客体访问权或部分访问权授予其他主体**  **强制访问控制：用户的权限和客体的安全属性都是系统管理员人为设置，或由操作系统自动地按照严格的安全策略与规则进行设置**  **访问权限的传递性**  **自主访问控制：具有某种访问能力的主体能够自主地将访问权的某个子集授予其它主体，权限具有传递性**  **强制访问控制：系统用该安全属性来决定一个主体是否可以访问某个客体，安全属性是强制的，任何主体都无法变更**  **安全性**  **自主访问控制安全性比强制访问控制弱**  **灵活性**  **自主访问控制灵活性比强制访问控制强**  **相同点在于**  **主要目标都是确保对系统资源的访问是受控的、合法的和安全的。**  **都使用访问控制规则来定义和管理对系统资源的访问。** |

5.（2014）安全风险评估时采用客观扫描工具除了网络扫描类之外，还有哪些类？实施扫描评估前要先评估扫描对目标系统可能产生的影响并做好适当的预防措施，这些影响一般有哪些？简述其主要部分。（15分）

|  |
| --- |
| **主机扫描工具：**主机扫描工具用于评估目标系统上主机的安全性。它可以检测操作系统和应用程序的漏洞、配置错误、未经授权的服务等问题，并提供修复建议。  **应用程序扫描工具：**应用程序扫描工具专门针对Web应用程序进行安全评估。它可以检测常见的Web漏洞，如跨站点脚本（XSS）、SQL注入、命令注入等，并提供修复建议。  **数据库扫描工具：**数据库扫描工具用于评估数据库系统的安全性。它可以检测数据库配置错误、权限问题、敏感数据泄露风险等，并提供修复建议。  **在评估扫描对目标系统可能产生的影响时，需要考虑以下几个方面的影响：**  **网络拥塞：**扫描过程可能会占用目标系统的带宽和网络资源，导致网络拥塞，影响正常的网络通信和业务运行。  **系统性能下降：**扫描过程可能会占用目标系统的计算资源和存储资源，导致系统性能下降，影响系统的响应时间和处理能力。  **服务不可用：**某些扫描活动可能会触发目标系统的安全防御机制，导致系统对扫描请求做出响应，甚至可能造成系统崩溃或服务不可用的情况。  **数据泄露风险：**扫描过程中可能会获取到目标系统的敏感信息或者产生敏感信息的副本，存在数据泄露的风险。  **为减轻这些影响，可以采取以下预防措施：**  与系统管理员或网络管理员协调，避免在高峰期进行扫描，以减少对网络性能的影响。  针对扫描前的目标系统进行备份，以防止数据丢失或损坏。  与目标系统的所有者和管理者协商并获得授权，确保扫描活动符合法律和组织的合规要求。  限制扫描范围，避免对生产系统或关键业务系统进行全面的扫描，而是选择有针对性的扫描策略。 |

6.（2014）阐述信息安全保障的CIA三角之C的主要两层含义。以一个学生成绩远程查询系统为例，具体分析其查询持续服务能力（a）可能面临的安全威胁和安全风险，并为此设计一个安全体系结构，请具体给出主要过程，如深度保护区划分和信息资产识别、威胁-脆弱性-安全风险分析、安全需求定义，安全策略设计、设计-组织和运行管理体系设计等。（20分）

P159+P176+P19

7.（2018）我国重要信息系统实行等级保护制度。等级保护第三级要求主机安全和应用安全均实现剩余信息保护。请以在一个windows服务器上运行的c++服务程序为例，说明什么是剩余信息保护、并具体描述一个如何在编程上实现对缓存上剩余信息保护的路径。（20分）。

8\*.（必考）针对同济大学校园网，分别从（a）学校总的视图，（b）嘉定校区管委会视图，画出“三保卫一支撑”四个区域的草图，并列表标出各区域的主要信息资产，并给定明确的域边界。从嘉定校区管委会的角度，分析同济大学校园网的通用安全、应用安全、服务安全，并给出通用安全体系结构描述的网络拓扑、应用安全和服务安全的逻辑拓扑。（20分）

作业2

9\*.阐述经典安全体系结构、IATF、等级保护2.0之间的关系。以同济大学校园卡充值系统为例，具体刻画保护目标，分析可能面临的安全威胁和安全风险，并为此设计一个安全体系结构。请给出主要过程，如刻画保护目标、识别细部区域的主要信息资产（并区分重要程度）、安全风险分析、安全需求定义，安全策略设计、应对的安全服务和安全机制等。（20分）

P159+P176+P19

|  |
| --- |
| 经典安全体系结构：经典安全体系结构是指传统的信息安全体系结构模型，通常包括安全策略、安全控制、安全运营和安全管理等组成部分。这种体系结构主要关注信息安全的整体框架和原则，通过制定安全策略、实施安全控制措施、建立安全管理体系等来保护信息系统的安全性。  IATF（Information Assurance Technical Framework）：IATF是由美国国家安全局（NSA）提出的一个信息保障技术框架，旨在指导和规范信息系统和网络的安全实施。IATF包含了一系列的技术要求、安全控制和评估方法，用于保障信息系统和网络的机密性、完整性和可用性。它提供了一套标准和指南，帮助组织实现信息安全目标。  等级保护2.0：等级保护2.0是中国国家标准化管理委员会发布的信息安全评估标准，是对之前的等级保护1.0进行升级和改进的版本。等级保护2.0通过对信息系统的评估和分类，提供了一套安全等级划分和安全控制要求，用于指导和规范信息系统的安全保护工作。它主要关注信息系统的机密性、完整性和可用性，根据信息系统的重要性和风险等级，提供了相应的安全要求和控制措施。 |

10\*.阐述剩余信息保护的含义。从安全机制的角度，阐述分级保护中第二级和第三级的三个区别。并分析数据结构如何支撑访问控制？对于一个具体的同济大学统一身份认证应用，从安全体系结构、数据安全角度、鉴别和访问控制分别分析二层和三层的优缺点。（20分）

|  |
| --- |
| 分级保护中第二级和第三级的区别：    安全要求：第二级和第三级在安全要求上有所不同。第二级相对于第三级来说，安全要求较低一些。第二级主要关注信息系统的机密性和完整性，要求实施一些基本的安全控制措施来保护系统中的敏感信息。而第三级则在第二级的基础上进一步加强了安全要求，要求实施更加严格的安全控制措施，同时还要考虑信息系统的可用性。  安全控制：第二级和第三级的安全控制措施也存在差异。第二级要求实施一些基本的安全控制措施，如访问控制、身份认证、加密传输等，以保护信息系统的机密性和完整性。而第三级在第二级的基础上增加了更多的安全控制措施，包括安全审计、安全监控、数据备份等，以提高信息系统的可用性。  风险评估：第二级和第三级的风险评估要求也有所不同。第二级要求进行风险评估，但强调以定性方法进行，即根据情况进行主观判断，并制定相应的风险应对措施。而第三级要求进行风险评估，并强调以定量方法进行，即通过数据和统计分析来评估风险，并制定相应的风险管理措施。  **优缺点：**  （1）安全体系结构：  第三级保护要求对系统进行更严格的安全设计和评估，能够提供更高级别的安全保障。  通过更严格的安全隔离和信息流控制，能够有效预防高级威胁和攻击。  强化的安全管理和安全审计机制，能够提供更高级别的安全性和可管理性。  （2）数据安全角度：  第三级保护要求对数据进行更严格的加密和完整性保护，能够提供更高级别的数据安全。  高级加密算法和密钥管理机制，能够防止高级攻击手段对数据的窃取和篡改。  数据备份、恢复和销毁等机制，能够提供数据的可靠性和可控性。  （3）鉴别和访问控制： |

11\*.简要介绍剩余信息保护（网络、主机、应用层面分别介绍）、强制访问控制、鉴权，针对某个应用的访问记录信息，从上述三个角度，分别给出它们在C++程序设计层面的至少一种解决方案。（15分）

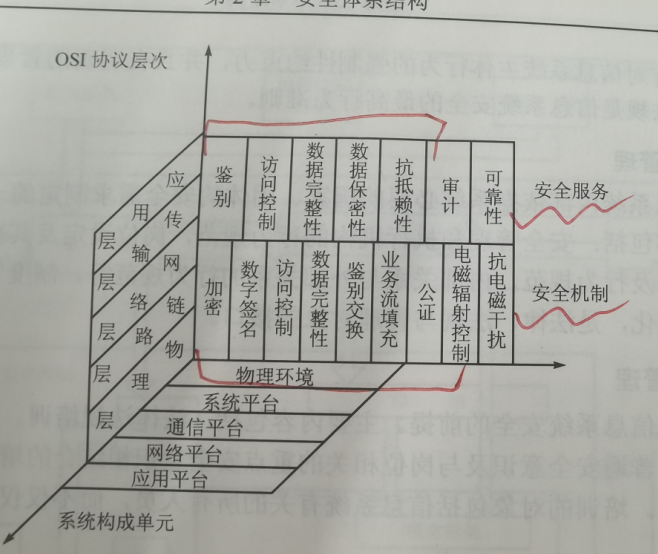
|  |
| --- |
| 剩余信息保护：  网络层面：  不可提供剩余信息保护  主机层面：    应用层面： |

12\*.（必考）简要介绍剩余信息保护中buffer的含义和作用，介绍如何清除静态存储信息、动态缓存信息、副本信息。（15分）

|  |
| --- |
| buffer缓冲区：一般情况下数据会先读到缓冲区，在读到缓冲区时，会在内存创建一个副本。  （1）静态存储信息：  对于静态变量，可以使用静态变量的赋值操作或者重新初始化静态变量。  （2）动态缓存信息：  释放内存，重写内存区域，或者将数据信息以不可理解的方式拆分到多个内存区域。  Windows API securememoryzero可以实现内存区域的重写覆盖。  （3）副本信息：  Windows API getfilemapped可以将文件直接映射到内存，从而实现不需要再读到缓冲区，就是不用在内存再创建副本。 |

13\*.（必考）对于同济大学成绩查询系统，分别从系统管理员、安全审计员、安全管理员、教务员、自身五个角度，分析：①如何保护数据的安全，②详细分析不同角度面临的安全风险，③从数据安全维度设计安全体系结构，④给出程序的操作。（20分）





**信息安全原理**

1.如何理解Ipsec安全联盟SA的本地化和单向性？在同一个节点设备上AH和ESP能共享同一个SA吗，为什么？为什么IPSec要对进入和外出两个方向的SA进行单独的控制？（15分）

|  |
| --- |
| 参考解答：  （1）如何理解Ipsec安全联盟SA的本地化和单向性：  安全关联是两个应用IPsec实体（主机、路由器）间的一个单工连接，决定保护什么、如何保护以及谁来保护通信数据。它规定了用来保护数据报安全的安全协议、密码算法、密钥以及密钥的生存期。SA是单向的，要么对数据报进行“进入”保护，要么对数据报进行“外出”保护。  （2）在同一个节点设备上AH和ESP能共享同一个SA吗，为什么：  不能共享。一个SA对IP数据报只能提供AH或ESP保护。  （3）为什么IPSec要对进入和外出两个方向的SA进行单独的控制：  进入和外出的数据的安全需求不同，一般对进入的数据安全要求更高，因此它们的安全处理未必相同，需要用不同SA处理。 |

2.简要介绍应用IPSec时，安全协议等参数的存储位置。阐述安全关联的字段。简要介绍IPSec AH/ESP。从实际部署角度，分析隧道/传输模式的异同。（15分）

|  |
| --- |
| 参考解答：  （1）应用IPSec时，安全协议等参数的存储位置：  若应用IPsec，策略要包含使用的安全协议（AH、ESP）、模式、算法等参数以安全关联的形式存储在SAD（security Association database）中。  （2）安全关联的字段包括：  目的IP地址（SA的目的地址，可为终端防火墙、路由器、系统等网络设备）、IPsec协议（标识用的AH还是ESP）、序号计数器（用于产生AH或ESP头的序号）、序号计数器溢出标志（若溢出，则产生一个审计事件，并禁止用SA继续发送数据报）、抗重放窗口（32bit计数器及位图，决定进入的AH或ESP数据报是否为重放的）、密码算法和密钥、安全关联的生存期。  （3）简要介绍IPSec AH/ESP：  AH对应IPsec数据交互阶段，AH只提供认证功能（数据源发认证和完整性校验），ESP同时提供机密性和完整性保护（机密性和认证服务），因为加解密操作是耗时的，所以在仅需要认证的场合就可以使用AH。  （4）从实际部署角度，分析隧道/传输模式的异同：  从部署方面看，IPsec有传输和隧道两种模式，在网关上使用IPsec时，通常使用隧道模式，当在两台主机上使用时，通常使用传输模式。 |

3.分析SSL防重放攻击的安全机制，并比较分析其与ipsec反重放机制的主要异同点。详细介绍ipsec反重放机制、SSL防重放机制。（20分）

|  |
| --- |
| 参考解答：  （1）SSL防重放攻击的安全机制：  SSL防重放是通过客户端（服务器）向服务器（客户端）发送随机数来实现，期待这个随机数两次是不同的，如果有两次随机数相同，则说明发生了重放攻击。  （2）与ipsec反重放机制的主要异同点：  Ipsec防重放是使用AH 或ESP中的序号，若两次序号相同，则发生了重放攻击。  （3）IPsec防重放攻击：  使用AH（ESP）保护数据发送接收数据的处理过程：  发送数据  ①查询SA以获取安全参数  ②（报文加密）  ③生成序号  ④计算认证数据  ⑤构造IPsec报文并发送  接收数据：  ①根据<SPI，目的IP地址，安全协议>在SAD中查找相应的SA，如果找不到就丢弃这个报文  ②使用滑动窗口机制验证序号，防止重放攻击  ③验证认证数据，若通过验证，则还原数据并递交给相应的协议模块或转发，否则丢弃报文（验证认证数据，验证失败则丢弃报文）  ④（解密，并将还原后的数据递交给相应的协议模块或转发，解密失败则丢弃报文）  （4）SSL防重放攻击：  SSL（安全套接层）标准规定了4个协议：握手协议（与SSL协商有关）、更改密码规范协议（与SSL协商有关）、警告协议（同时包含SSL安全通道关闭及错误通告功能）、记录协议（数据封装和处理）。  SSL提供的安全服务：机密性、完整性、服务器认证以及可选的客户端认证。  客户端想服务器发送ClientHello消息，其中包含了客户端所支持的各种算法和一个随机数，这个随机数将用于各种密钥的推导，并可以防止重放攻击。  服务器端返回ServerHello消息，随机数的功能与上述相同。  警告协议包括两种功能：一是提供了报错机制，即通信双方若某一方法发现了问题便会利用该协议通告对等段；二是提供了安全断连机制，即以一种可认证的方式关闭连接。 |

4.从适用场景、安全机制、能对抗的安全威胁等方面（至少包括、但不限于），具体比较分析L2tp用户认证与PGP认证的实现原理和安全性。（15分）

|  |
| --- |
| 参考解答：  （1）L2tp用户认证的实现原理和安全性：  LAC：L2TP接入集中器；LNS：L2TP网络服务器  远程系统的PPP帧首先发送给LAC，LAC将它作为L2TP协议报文的数据区封装并发送给LNS，LNS则对报文进行解封处理后发送给家乡网络中的主机。某些情况下，主机可以不依赖LAC，而是独立运行L2TP，并于LNS建立隧道。  数据消息：通过数据通道传输，不保证数据的可靠传输，承载PPP帧。  控制消息：通过控制通道传输，保证控制消息的可靠传输，用于L2TP隧道和会话的协商及维护。  L2TP基于UDP。L2TP包括两种消息，数据消息和控制消息，分别通过数据通道和控制通道传输，L2TP不保证数据消息的可靠传输，但保证控制消息的可靠传输。L2TP不提供对PPP数据的机密性和完整性保护，若使用CHAP，则可体现端点身份认证的功能。  L2TP规定了以下确保控制消息的可靠投递的机制：  ①每个L2TP 报文都包含序列号，从而为监测报文丢弃和乱序提供了基础  ②L2TP使用肯定确认防止报文丢弃，即接收方收到报文后发回确认。发送发若在一段时间之内没有手动啊确认则重发  ③L2TP使用滑动窗口技术提高通信效率并进行流量控制  ④L2TP使用慢启动策略防止拥塞  （2）PGP认证的实现原理和安全性：  数字签名:DSS/SHA或RSA/SHA  完整性：RSA、MD5  消息加密:CAST-128或IDEA或3DES + Diffie-Hellman或RSA  数据压缩:ZIP  邮件兼容:Radix 64(将任意二进制输入，转换成可打印的字符输出的编码技术)  数据分段：大邮件自动分段并在接收时自动恢复。  ·身份鉴别    ·保密性    发生在签名后、加密前。  压缩    压缩发生在签名后，加密前 |

5.考虑如下图所示的原始应用环境，A是远程工作前端网络的接入网关，C是后台业务资源网的接入网关。前述两个网内部IP分配均是独立的私网地址，A与C之间为第三方IP网络，其间可能存在NAT、或代理、或端口控制等环节。

****

上图所示网络环境中，请注意B所在网段有网关A和无线网关W两个出口。

需要从B-C建立端-gate的IPSEC通道、并屏蔽W带来的不确定性，如何建立B-C的ipsec SA安全联盟？

（1）请给出各种可能的sa组合；

（2）并从中挑选出符合要求的ipsec sa隧道配置方案，并给出理由；

（3）比较分析各种可能的组合各自存在的主要安全风险、以及对抗安全威胁能力的区别。（25分）

|  |
| --- |
| 参考解答：  （1）在不考虑可行性和正确性的前提下，各种可能的SA组合如下所示：  A-C：①AH隧道；②ESP隧道；③ESP and auth隧道；④AH+ESP隧道；⑤AH+ESP and auth隧道；⑥AH传输；⑦ESP传输；⑧ESP and auth传输；⑨AH+ESP传输；⑩AH+ESP and auth传输。  A-B：①AH隧道；②ESP隧道；③ESP and auth隧道；④AH+ESP隧道；⑤AH+ESP and auth隧道；⑥AH传输；⑦ESP传输；⑧ESP and auth传输；⑨AH+ESP传输；⑩AH+ESP and auth传输。  B-C：①AH隧道；②ESP隧道；③ESP and auth隧道；④AH+ESP隧道；⑤AH+ESP and auth隧道；⑥AH传输；⑦ESP传输；⑧ESP and auth传输；⑨AH+ESP传输；⑩AH+ESP and auth传输。  在上面的基础上，SA组合为：“A-C、A-B”、“A-C、B-C”。  （2）符合要求的ipsec sa隧道配置方案及其理由：  ①分析不同的路线、方式、嵌套关系：  由于B所在网段有网关A和无线网关W两个出口，要想实现排除无线网关W带来的不确定影响，应当在A-B或者B-C配置ipsec sa。在A或C配置访问控制。  ②讨论可连接性和使用原因：  由于B为私有网络，无法直接路由，考虑可连接性，应当在A-C配置ipsec sa。  ③分析隧道模式或传输模式等的选择依据：  由于A、C均为网关，A-C应为隧道模式。A-B为端到端连接，可选隧道或传输模式。B-C为网关-端连接，应为隧道模式。  （3）①“A-C、A-B”1+2 本地化拼接 建立时把别人的全部屏蔽掉，所有错误都在本地，出错小，如果网关信息泄露，会增大损失  ②“A-C、B-C”1+2 交叉拼接 信息扩散少 不会让自身SA听到  +AH/ESP 的优缺点 |
| 传输模式用于两台主机之间的通讯，或者是一台主机和一个安全网关之间的通讯。在传输模式下，对报文进行加密和解密的两台设备本身必须是报文的原始发送者和最终接收者。换句话说，就是加解密点是实际的通信点。正是因为如此，如果通信双方的IP地址是私网地址，那么该VPN无法穿越Internet。 |
| ①1+1 信息泄露少  ②1+2 本地化拼接 建立时把别人的全部屏蔽掉，所有错误都在本地，出错小，如果网关信息泄露，会增大损失  ③1+2 交叉拼接 信息扩散少 不会让自身SA听到 |

6.考虑如下图所示的原始应用环境，A是远程工作前端网络的接入网关，C是后台业务资源网的接入网关。前述两个网内部IP分配均是独立的私网地址，A与C之间为第三方IP网络，其间可能存在NAT、或代理、或端口控制等环节。

****

考虑基于**PGP和pop3/SMTP基本邮件服务**以附件形态从B到D传输**大**数据文件，**基于PGP**保证其间数据的机密性和完整性，考虑把B端CPU序列号和操作系统及用户注册信息等本地软硬件环境参数的md5值作为端端识别参量，如何与大数据文件一起打包后（请具体画出封包形式）经pgp处理后传到D端以认证B设备？画出从B端原始文件、到发送端处理、邮件发送、D端接收、接收端认证和数据还原处理等主要操作流程，以及发送端和接收端对应的端认证过程。（25）

|  |
| --- |
| 参考解答：  PGP的实际操作由五种服务组成：鉴别、机密性、电子邮件的兼容性、压缩、分段和重装。  PGP（Pretty Good Privacy）：是一个可提供机密性和认证的软件。通常用来加密和解密电子邮件。    Md5用作单向hash函数，通过使用RSA算法加密，用邮件发送者的秘密钥对md5消息摘要进行加密。  字母和符号的含义如下：  Ks : session key  KRa : 用户A的私钥  KUa : 用户A的公钥  EP : 公钥加密  DP : 公钥解密  EC : 常规加密  DC : 常规解密  H : 散列函数  || : 连接  Z : 用ZIP算法数据压缩  R64 : 用radix64转换到ASCII格式  PGP消息产生过程：    PGP消息接收过程： |

6.分析安全协议在TCP/IP协议栈的分布。（10分）

|  |
| --- |
| 参考解答：  应用层：L2TP、SSH（基于TCP）、PGP、IKE  传输层：SSL、Socks  IP层：IPSec  L2TP：不提供机密性（没有对数据的加密功能），  IPsec：身份认证、机密性、完整性和防止重放攻击  IKE的功能包括SA协商、密钥生成和身份认证，它是一个应用层协议基于UDP。  身份认证(IKE，通信双方互相认证)  数据源发认证(AH、ESP)  完整性（AH、ESP）  防止重放攻击（AH、ESP）  机密性(ESP+传输模式、ESP+隧道模式)  对通信流提供有限的机密性保护(ESP+隧道模式)  SA提供的安全服务取决于所选的安全协议（AH或ESP）、SA模式(传输或隧道)、SA作用的两端点  SSL（TLS）：为两个通讯个体之间提供机密性、完整性，服务器认证以及可选的客户端认证。  服务器身份认证：典型流程  客户端身份认证：客户端认证流程，可选  完整性：Finished消息（防止降级攻击）  机密性：记录协议中定义  安全断连：Close notisfy消息  SSH：机密性、完整性保护、身份认证（必选的服务器认证，可选的客户端认证）  服务器身份认证：传输层协议，必选的  客户端身份认证：用户认证协议，可选的  完整性：传输层协议定义  机密性：传输层协议定义  防止重放攻击： SG\_MSG\_KEXINIT消息中包含的cookie  SSH传输协议(协商和数据处理，包含服务器身份认证)：  SSH通信总是由客户端发起。当期望使用SSH时，客户端首先通过三次握手与服务器的22号端口建立TCP连接。  ①版本协商  ②密钥交换：  (1)算法协商  (2)D-H交换：实现了密钥交换、服务器身份认证、握手消息完整性验证  防重放攻击：SSH\_MSG\_KEXINIT消息中包含的cookie是一个随机数，在计算密钥和生成会话ID时它是输入之一。每次安全协商时应选取不同的cookie值，所以如果两次协商所获取得会话ID相同，则有可能发生了重放攻击。  (3)计算密钥  ③服务请求/响应  ·SSH传输层协议与用户认证协议的关系如何?  传输层协议只提供服务器认证功能，没有用户认证功能，如果需要认证用户身份，则客户需要利用传输层协议向服务器提出用户身份认证服务请求，若服务器接受请求，则双方开始执行SSH身份认证协议。  身份认证协议在传输层协议提供的安全通道上运行。  ·SSH连接协议  当客户端通过SSH传输层协议发出连接协议服务请求后，即可开始连接协议相关的流程。该协议规定了利用SSH传输层协议已建立的安全通道进行交互式登录会话、远程执行命令、转发TCP/IP连接记忆X11连接的相关内容。传输层协议构建的安全通道成为隧道，而所有的终端绘画和被转发的连接都被陈伟通道。一条隧道可以包含多条通道，这意味着SSH安全协议可以同时为多个不同的应用提供安全服务。  代理安全Socks（防火墙安全会话转换协议）  ·使用端口1080，工作于应用层。  ·可转发所有高层应用，对操作系统无限制。  ·专门设计用于防火墙  ·在应用层和传输层之间垫了一层  ·Socks库和sockd守护程序  ·不支持ICMP转发  Socks本身未定义机密性、完整性保护方法，但由于所有通信量都要经过代理服务器转发，为统一制定安全策略并部署安全防护措施提供了便利。  Socks 5支持多种客户端身份认证方案，如果某些认证方案能够支持机密性和完整性保护，这些功能在应用Socks后仍然能够得到保留。  ·Socks客户端命令：  CONNECT：通告代理服务器与远程主机建立连接，调用函数：Rconnect  BIND：通告服务器接收来自某个远程主机的连接请求，调用函数：Rbind，Rlisten和Raccept.  ·Socks 5沿袭了Socks 4的体系结构以及命令，并作了以下扩展  1.扩展了客户端身份认证功能，支持多种身份验证方法：用户名/口令认证方法（用户名和口令以明文方式发送，如被截获面临身份被假冒的风险）、GSSAPI认证（GSSAPI为定义所使用的认证方法和密钥交换方法，其安全风险取决于所使用的认证方法和密钥交换方法的安全性）。  2.扩展了寻址方法：除了IPv4地址外，还支持域名及IPv6地址（基于Socks的IPV4/IPv6网关）  3.增加了对UDP的支持 |

7.比较SSLv3与IPSec，请从功能的角度分析这两个协议套件所包含的安全协议之间的对应关系。（10分）

|  |
| --- |
| 参考解答：  ·密码算法和密钥协商：SSLv3的握手协议，IPSec的IKE协议  ·差错通知、状态通知：SSLv3的警告协议，IPSec的IKE协议的通知交换模式  ·消息完整性：SSLv3记录格式中的MAC，IPSec的AH和ESP报文中的认证数据。  ·加密：SSLv3的记录协议，IPSec的ESP  ·身份认证：SSLv3握手协议，IPSec的IKE |

8.利用SSL也可以构建VPN，但IPSec VPN仍然是企业解决方案主流，为什么？（10分）

|  |
| --- |
| 参考解答：  **·SSL VPN只能进行认证和加密，不能实施访问控制**，建立隧道后，管理员对用户不能进行所有的控制，而集成防火墙的IPSec VPN则可以根据用户的身份和角色进行安全控制和审计。  **·SSL VPN局限了用户只能访问web服务器的应用，**而IPSec VPN几乎能为所有应用提供访问。  **·SSL VPN只提供了单一的证书认证方式**，企业需要购买或者部署一个小型证书系统，IPSec可以提供多种认证方式。  ·SSL VPN位于传输层，IPSec VPN位于网络层，SSL VPN的**效率**比IPSec VPN 差。  ·要实现**网络-网络的安全互联**，只能考虑使用IPSec VPN。 |

9.从配置方法、管理简易性、可扩展性和安全性等方面对SSL VPN与SSH VPN进行比较。（10分）

|  |
| --- |
| 参考解答：  ·效率：SSH位于TCP/IP协议栈的应用层，SSL位于传输层，利用SSH构建VPN比SSL消耗更多带宽。  ·配置方法：SSH VPN使用TCP/IP端口转发，SSL VPN使用分设端口。  ·管理简易性：使用上，SSL VPN对用户完全透明，SSH VPN需要用户登录到用户账户上。管理上，SSH VPN可配置成仅允许目标端口为22的通信量通过，配置和管理更加简单，而SSL VPN对不同应用的访问端口不同。  ·可扩展性：SSH不支持UDP和ICMP报文，SSL不支持UDP报文但支持ICMP报文。  ·安全性：SSH VPN和SSL VPN都提供了机密性、完整性和身份认证功能，他们支持的密码算法不同。 |

10.SSH用户协议支持基于口令的认证方法，且不对口令作加密处理。它这样放心地传输口令的依据是什么？（5分）

|  |
| --- |
| 参考解答：  SSH的身份认证协议在传输协议所建立的安全通道上进行。身份认证协议的报文封装在传输协议的报文的数据区中，而传输协议的报文的数据区可以进过加密处理后发出去，所以身份认证协议的数据可以以明文形式发送而无需关心保密性。 |

11.如果通信双方都具备IPv4和IPv6协议栈6网络，假设发起方连接IPv6网络，回应方连接IPv4，中间是Socks网关，请写出回应方向发起方发送的报文的发送过程。（5分）

|  |
| --- |
|  |

12\*.（必考）阐述ssh两层三个协议和tls两层四个协议的主要内容，分别介绍它们的安全服务和安全机制是在何处实现的。给定一个ssh服务器，要想认证终端真伪有几种方式？要想达到等级保护第三级，给出实现的三种基本方式，同时给出一个可行的复杂组合方式。（20分）

|  |
| --- |
| IMG_256  （1）SSH（Secure Shell）协议是用于安全远程访问和管理计算机系统的协议。它主要包括以下三个协议：  SSH-TRANS：传输层协议，用于提供安全的数据传输功能。它使用加密和身份验证机制来保护数据的机密性和完整性，防止数据被篡改和窃取。  SSH-USERAUTH：用户身份验证协议，用于验证用户的身份。它支持多种身份验证方法，包括密码、公钥、证书等方式。  SSH-CONNECTION：连接协议，用于管理SSH连接。它支持会话管理、通道管理、环境变量设置等功能，提供了灵活的连接管理功能。  （2）TLS  Handshake Protocol：握手协议，用于建立安全连接。客户端和服务器之间通过该协议进行身份验证、密钥协商、协议版本协商等操作，以建立安全的通信连接。  Change Cipher Spec Protocol：变更密码规范协议，用于告知对方后续加密通信所使用的密码规范。当双方都接受对方的身份验证并协商出一致的加密算法和密钥后，就可以使用该协议告知对方后续通信所使用的密码规范。  Alert Protocol：警报协议，用于在通信过程中传递警报信息。当出现安全性问题或通信异常时，该协议可以向对方发送警报信息，以及断开连接等操作。  Record Protocol：记录协议，用于对传输的数据进行加密和认证。该协议将应用层数据分割成多个记录，并对每个记录进行加密和认证，以保证数据的机密性和完整性。  这三个协议共同构成了SSH协议的核心部分，提供了安全和可靠的远程访问和管理功能。在实际应用中，SSH协议通常被用于远程登录、文件传输、远程执行命令等场景。  SSH是Secure Shell的缩写，主要用于远程登录和数据传输加密。SSH由两部分组成：SSH传输层协议和SSH用户身份验证协议。SSH传输层协议包括SSH连接协议和SSH会话协议两个协议层。SSH用户身份验证协议包括用户身份验证请求、用户身份验证响应、用户身份验证成功和用户身份验证失败四个协议。  SSH的安全服务主要包括身份验证，加密和完整性保护。身份验证主要用于验证客户端和服务端的身份，防止非法访问。加密主要用于保护数据的机密性，防止数据被窃听。完整性保护主要用于保护数据的完整性，防止数据被篡改。  SSH的安全机制一部分实现在传输层协议中，另一部分实现在用户身份验证协议中。传输层协议中使用了公钥加密和对称加密算法来保护数据的机密性和完整性，同时也使用了数字签名算法来验证数据的来源和完整性。用户身份验证协议中通过使用密码和公钥等方式来验证客户端和服务端的身份。  TLS是Transport Layer Security的缩写，是一种安全传输协议，用于保护网络通信的安全性。TLS由两部分组成：TLS协议和TLS握手协议。TLS协议包括记录协议、警告协议和握手协议三个协议层。TLS握手协议包括客户端和服务端之间的握手过程和密钥协商过程。  TLS的安全服务主要包括身份验证，加密和完整性保护。身份验证主要用于验证客户端和服务端的身份，防止非法访问。加密主要用于保护数据的机密性，防止数据被窃听。完整性保护主要用于保护数据的完整性，防止数据被篡改。  TLS的安全机制主要实现在记录协议、握手协议和密钥协商过程中。记录协议主要使用对称加密算法和MAC算法来保护数据的机密性和完整性。握手协议主要使用非对称加密算法和数字签名算法来保证通信双方的身份验证和密钥协商的安全性。密钥协商过程主要使用Diffie-Hellman密钥交换算法来协商对称加密算法的密钥。 |

13\*.（必考）综合题。（ipsec层面、sock层面、ssh层面）

（1）假定要想实现访问控制，从ipsec层面（OSI 3层）、sock层面（OSI 5层）、ssh层面（OSI 7层）分别介绍实现方法，并总结不同点。

（2）假设攻击者窃听、中间人攻击两种情形，在上述三种层面如何防范？如何组合？

（3）对于重放攻击，在第二层、第三层、第四层如何部署反重放攻击？

（4）以第三层为例，ipsec反冲放攻击有几种机制，它是在ipsec的哪个层面做的工作（ah还是esp）？简要阐述原因。

（5）sock的反重放攻击是在哪个层面实现的？简要介绍recalled反重放机制提供的两个基础服务，及其反重放机制的实现方法。对于同一个终端有多个sock/多个窗体，它们并行且也是互相隔离的，它的基本原理是什么？

（6）对于同济大学嘉定校区，请分析需要保护的目标（信息资产识别）、保护环境、安全威胁（多种）、安全威胁在何时可以成功防范？何时不可以成功防范？使用哪些安全策略？使用什么安全服务？用什么机制实现安全服务？（25分）

|  |
| --- |
| （1）  IPSec：IPSec 是一种在 IP 层面上提供安全性的协议，它可以通过对数据包进行加密、认证和完整性保护来保障通信的安全性。在实现访问控制方面，IPSec 可以通过对**数据包进行过滤**，只允许符合规则的数据包通过，从而达到访问控制的目的。IPSec 的过滤规则包括源地址、目的地址、协议类型、端口号等多个因素，可以根据实际需要进行配置。  SOCKS：SOCKS 是一种用于网络代理的协议，它可以通过代理服务器来实现访问控制。在 SOCKS 中，代理服务器会对客户端发起的所有连接进行**验证和授权**，只有授权的连接才能通过代理服务器进行访问。SOCKS 的访问控制主要基于用户身份认证和授权，可以通过配置用户名和密码等信息来控制用户的访问权限。  SSH：SSH 是一种用于安全远程登录的协议，它可以通过加密和身份验证来保障登录的安全性。在实现访问控制方面，SSH 可以通过**配置访问控制列表（ACL）**，只允许符合 ACL 规则的用户进行登录。SSH 的 ACL 规则可以基于 IP 地址、用户名、时间等多个因素进行配置。  总体来说，IPSec、SOCKS、SSH 三者的访问控制方法存在一些差异。IPSec 主要通过过滤数据包来实现访问控制，SOCKS 主要通过代理服务器来实现访问控制，SSH 主要通过 ACL 规则来实现访问控制。此外，IPSec 和 SOCKS 主要用于网络层面上的安全，而 SSH 主要用于应用层面上的安全。  （2）【中间人攻击】  IPSec协议可以通过使用**数字证书、预共享密钥**等方式对通信双方进行身份认证，并使用密钥协商机制确保通信双方的通信密钥安全性，从而防范中间人攻击。在IPSec的VPN场景下，还可以通过在VPN客户端和VPN网关之间建立隧道，对通信进行加密和完整性保护，从而进一步增强安全性。  SOCKS协议可以通过使用**身份验证和加密等机制**对客户端与SOCKS代理之间的通信进行保护，从而防止中间人攻击。SOCKS5协议支持多种身份验证方式，包括无验证、用户名密码认证、GSS-API认证等，可以根据实际需要进行选择。  SSH协议可以通过使用**公钥认证、主机密钥认证**等方式对SSH客户端和SSH服务器进行身份认证，并使用加密和完整性保护机制，防范中间人攻击。在SSH的端口转发和隧道场景下，还可以通过使用SSH端口转发和SSH隧道等功能，将明文流量通过加密的SSH通道进行传输，从而增强安全性。  （3）【反重放攻击】  IPSec协议使用ESP协议提供数据完整性、加密和反重放攻击保护。在IPSec协议中，ESP通过使用ESP头和ESP尾加密和完整性保护数据包。ESP头中包含了ESP的一些参数和SPI（Security Parameters Index）值，用于标识该数据包所使用的安全参数。ESP尾包含了对数据包的完整性校验值。  反重放攻击是指攻击者在网络上重放已经被传输的数据包，从而达到窃取信息或者攻击的目的。在IPSec中，反重放攻击的实现依赖于ESP头中的Sequence Number和Anti-Replay Window机制。  Sequence Number用于标识数据包的顺序，每个数据包都有一个独一无二的Sequence Number。接收方通过检查Sequence Number的值，可以判断是否收到重复的数据包或者数据包的顺序被篡改。  Anti-Replay Window机制通过维护一个滑动窗口，来检查并防止重复的和过期的数据包。滑动窗口中存储了已经收到并通过校验的数据包的Sequence Number值。当接收方收到一个新的数据包时，首先检查其Sequence Number是否在窗口中，如果不在，则接收方认为该数据包是重复的或者已经过期的数据包，将其丢弃。如果Sequence Number在窗口中，则接收方接受该数据包并将其加入到滑动窗口中，同时将窗口向前滑动一格。  通过Sequence Number和Anti-Replay Window机制，IPSec协议可以有效地防范反重放攻击。攻击者即使窃取了已经传输的数据包，也无法对其进行重放攻击，因为接收方会在Anti-Replay Window机制的限制下拒绝重复和过期的数据包。  （4）ESP 因为ah不会传递用户载荷。  （5）在socks中，为了保证数据包的安全性，可以使用recalled反重放机制提供的两个基础服务：会话标识和时间戳。其中，会话标识是指每个数据包都必须包含一个唯一的ID，而时间戳则是指每个数据包都必须包含一个当前的时间戳，以确保数据包的时序性。  recalled反重放机制的实现方法是通过在每个数据包中嵌入一个唯一的ID和当前的时间戳来实现。在收到一个数据包时，socks服务器会首先检查该数据包的ID是否已经出现过，如果出现过，则说明该数据包是一个已经被重放的数据包，应该被丢弃；如果没有出现过，则说明该数据包是一个新的数据包，应该被接受并缓存起来。同时，socks服务器还会检查该数据包的时间戳是否比之前接收到的数据包的时间戳晚，如果晚，则说明该数据包是一个新的数据包，应该被接受并缓存起来；如果早，则说明该数据包是一个已经被重放的数据包，应该被丢弃。  对于同一个终端有多个sock或多个窗口的情况，其基本原理是每个sock或窗口都有自己独立的进程或线程来处理输入输出操作，这些进程或线程之间是互相隔离的，因此可以并行处理多个输入输出操作。 |

14\*.（必考）对于同济大学校园网，如何排除想要接入的Wifi的影响？请配置合理的SA组合，要求不能产生新的风险、不能妨碍其他的任务，并分析通过SA做访问控制时，先后做了哪些工作。请以ipsec为讨论对象，做SA组合，分析不同的路线、方式、嵌套关系，讨论可连接性和使用原因，分析隧道模式或传输模式等的选择依据，给出你的结论。（25分）

见5

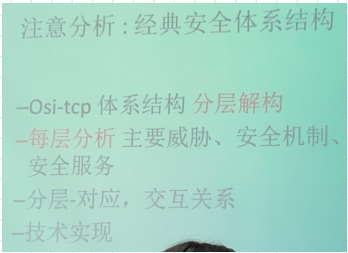
15\*.（必考）综合题。（终端安全）

对于同济大学邮件系统的储存业务，在考虑其存在的嵌套关系和持续关系的前提下，基于pgp，设计符合应用需求的协议。请给出：①给出先后分别需要做哪些工作，②传输数据的定义，③状态关联（哪些状态正常、哪些状态不正常、不正常如何处理），④定义工作流程，⑤定义结构关系（语义、数据结构和说明），⑥定义治理规则（是否正常工作的状态监控）。注意：对于此业务的不同操作，需分别按照上述步骤进行详细设计。（25分）

【协议四个方面】

|  |
| --- |
| GPT作答：  本次设计的协议基于pgp，旨在满足同济大学邮件系统的储存业务需求。具体设计如下：  工作流程  ① 发件人对邮件内容进行加密和签名  ② 发件人将加密和签名后的邮件发送给邮件服务器  ③ 邮件服务器将接收到的邮件存储在数据库中  ④ 收件人登录邮件服务器，并从数据库中读取邮件  ⑤ 收件人对邮件进行验证和解密，获取邮件内容  传输数据的定义  邮件数据在传输过程中需要进行加密和签名，确保数据的机密性和完整性。具体传输的数据包括邮件内容、加密后的邮件内容、签名、密钥等。  状态关联  正常状态：邮件内容加密和签名成功，邮件存储成功，邮件解密和验证成功。  不正常状态：邮件内容加密或签名失败，邮件存储失败，邮件解密或验证失败。  处理方法：对于不正常状态的邮件，需要及时通知发件人或收件人，并提供相应的处理方法。  定义结构关系  数据结构：  邮件内容：包括邮件主题、发件人、收件人、邮件正文等信息。  加密后的邮件内容：使用pgp协议对邮件内容进行加密，确保邮件的机密性。  签名：使用pgp协议对邮件内容进行签名，确保邮件的完整性。  密钥：用于加密和解密邮件内容，以及签名和验证邮件内容。  说明：  邮件内容和加密后的邮件内容是一一对应的，签名是对加密后的邮件内容进行的，密钥用于加密、解密、签名和验证。  定义治理规则  监控正常工作状态的方法：  ① 对于邮件发送和接收的每个步骤，都进行日志记录和监控，及时发现异常情况。  ② 对于邮件内容的加密、签名、解密和验证等操作，需要进行严格的权限控制，确保只有授权用户能够进行操作。  ③ 对于邮件内容的存储，需要进行备份和恢复，确保数据的可靠性和完整性。  以上是本次设计的协议，可以满足同济大学邮件系统的储存业务需求。在实际应用中，还需要不断地进行监控和优化，以提高系统的稳定性和安全性。 |

16.



17.

\* OSI 7 层各层能否 / 如何实现访问控制；

\* SSL 协议体系结构与记录协议安全机制默写，分析记录协议中的某安全机制具体实现；

|  |
| --- |
| SSL：握手、密码、警告、记录    记录协议的安全机制  将应用数据分割为多个片段；对每个片段进行压缩，**加上片段编号(防止重放攻击)**  **计算消息验证码MAC值(保证数据完整性)追加在压缩片段**  **对称密码加密，保证了消息的机密性** |

\* IPSec 与 SSL 在抵抗中间人攻击方面的对应策略；

\* IPSec 网关内主机到另一网关的通信如何屏蔽外部无线 AP 带来的安全风险；

\* 基于 PGP、SMTP/POP3 的带大数据附件邮件处理、发送、接受、认证、还原以及端端密钥注册交换流程。

|  |
| --- |
| （5）  PGP（Pretty Good Privacy）是一种加密通信协议，它可以用于保护电子邮件的隐私和安全。PGP可以用于处理、发送、接受、认证和还原带有大数据附件的邮件，并提供端对端的密钥注册和交换流程，具体步骤如下：  处理邮件：PGP可以对待发送或接收的邮件进行加密、签名、压缩等处理。用户可以使用PGP软件将需要发送或接收的邮件进行处理，例如通过PGP加密算法对邮件内容进行加密，使用PGP数字签名算法对邮件进行签名等。  发送邮件：PGP处理后的邮件可以通过标准的电子邮件协议（如SMTP）发送。在发送邮件时，用户需要将PGP处理后的邮件内容和附件发送给收件人的邮箱。  接收邮件：当收件人收到PGP处理后的邮件时，可以使用PGP软件对邮件进行解密、验签等操作，以还原邮件的原始内容。用户需要在PGP软件中输入自己的密钥来解密邮件。  认证邮件：PGP可以使用数字签名算法来对邮件进行认证，以确保邮件的发送者真实可信。在发送邮件时，用户可以使用PGP的数字签名算法对邮件进行签名，以证明邮件的真实性和完整性。在接收邮件时，用户可以使用PGP软件对邮件进行验签，以确保邮件的真实性和完整性。  端对端密钥注册和交换：PGP可以使用公钥加密算法来实现端对端的密钥注册和交换。在注册时，用户需要生成自己的公钥和私钥，并将公钥发布到密钥服务器上。在交换时，用户可以使用对方的公钥对发送的邮件进行加密，从而实现端对端的安全通信。  总之，PGP可以提供安全的电子邮件通信，保护邮件的隐私和安全，同时提供端对端的密钥注册和交换流程，确保通信的安全性。 |