第 16 章安全性和保密性

16.1 加密和解密

1. 【2009 年题 52 解析】

公司总部与分部之间通过 Internet 传输数据，需要采用加密方式保障数据安全。加密算法中，对称加密比非对称加密效率要高。RSA 和 ECC 属于非对称加密算法，MD5 为摘要算法，故选择 RC-5。

2. 【2016 年题 38 解析】

DES 加密算法的密钥长度为 56 位，三重 DES 要用到 2 个 DES 的密钥，所以长度为 112 位。

16.2 数字签名与数字水印

1. 【2018 年题 38 解析】

消息摘要是用来保证数据完整性的。传输的数据一旦被修改那么计算出的摘要就不同，只要对比两次摘要就可确定数据是否被修改过。因此其目的是为了防止发送的消息被篡改。

对摘要进行加密的目的是防止抵赖。

答案 CB。

16.3 数字证书与密钥管理

1. 【2012 年题 8 解析】

在 PKI 系统体系中，证书机构 CA 负责生成和签署数字证书，注册机构 RA 负责验证申请数字证书用户的身份。

【答案】A、B。

2. 【2013 年题 35 解析】

Kerberos 可以防止偷听和重放攻击，保护数据的完整性。Kerberos 的安全机制如下。AS(Authentication Servet)：认证服务器，是为用户发放 TGT 的服务器。 TGS(Ticket Granting Server)：票证授予服务器，负责发放访问应用服务器时需要的票证。认证服务器和票据授予服务器组成密钥分发中心(Key DistributionCenter，KDC)。 V：用户请求访问的应用服务器。TGT(Ticket Granting Ticket)：用户向 TGS 证明自己身份的初始票据，即 KTGS(A，KS)。 公钥基础结构(Public Key Infrastructure，PKI)是运用公钥的概念和技术来提供安全服务的、普遍适用的网络安全基础设施，包括由 PKI 策略、软硬件系统、认证中心、注册机构(Registration Authority，RA)、证书签发系统和 PKI 应用等构成的安全体系。

16.4 网络安全协议

1. 【2011 年题 47 解析】

在网络管理中要防止各种安全威胁。安全威胁分为主要和次要两类，其中主要的威胁有：

(1)篡改管理信息：通过改变传输中的 SNMP 报文实施未经授权的管理操作。

(2)假冒合法用户：未经授权的用户冒充授权用户。

企图实施管理操作次要的威胁为：

(1)消息泄露：SNMP 引擎之间交换的信息被第三者偷听。

(2)修改报文流：由于 SNMP 协议通常是基于无连接的传输服务，重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。

另外有两种威胁是安全体系结构不必防护的，因为不重要或者是无法预防。

(1)拒绝服务：因为很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全系统不必采取措施。

(2)通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息。

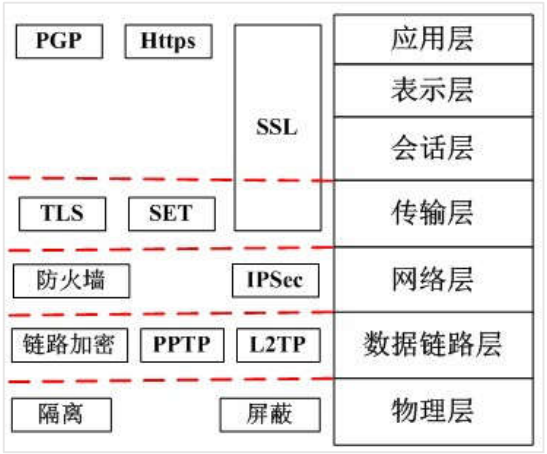
【答案】B。

2. 【2011 年题 48 解析】

PGP (Pretty Good Priracy)是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。PGP 并没有使用什么新的概念，它只是将现有的一些算法(如 MD5、RSA 及 IDEA)等综合在一起而已。PGP 提供数据加密和数字签名两种服务。

【答案】C。

3. 【2014 年题 43 解析】



【答案】A。

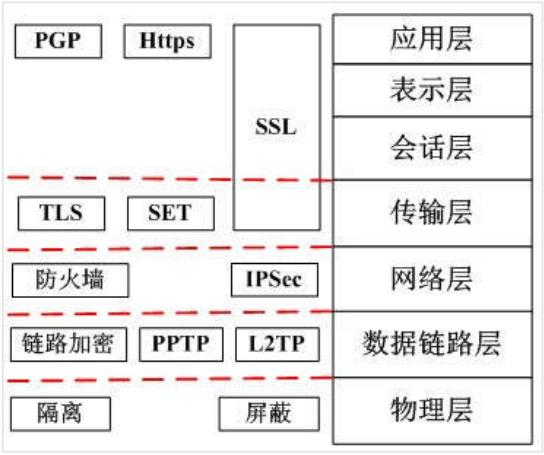
4. 【2017 年题 10 解析】

MIME(Multipurpose Internet Mail Extensions)中文名为：多用途互联网邮件扩展类型。S/MIME (Secure Multipurpose Internet Mail Extensions)是对 MIME 在安全方面的扩展。它可以把 MIME 实体(比如数字签名和加密信息等)封装成安全对象。增强安全服务，例如具有接收方确认签收的功能，这样就可以确保接收者不能否认已经收到过的邮件。还可以用于提供数据保密、完整性保护、认证和鉴定服务等功能。

S/MIME 只保护邮件的邮件主体，对头部信息则不进行加密，以便让邮件成功地在发送者和接收者的网关之间传递。

【答案】：D。

扩展：



5. 【2017 年题 40 解析】

IDS：即入侵检测系统，这个系统会根据操作行为的特征或是异常行径来判断，是不是一次入侵行为。像杀毒软件就用到了入侵检测系统的原理，通过特征识别病毒。

防火墙：作用是内外网之间的隔离。外网的请求要到内网，必须通过防火墙，所以防火墙能使用一些判断规则来把一些恶意行为拒之门外。但如果攻击本身来自内网，防火墙就无能为力了。

网闸：一个物理离隔离装置，与 IDS 与防火墙不同，网闸连接的两个网络是不相通的。网闸与内网相联时，会断开与外网的连接，与外网相联时，会断开与内网的连接。

UTM 安全设备的定义是指一体化安全设备，它具备的基本功能包括网络防火墙、网络入侵检测/防御和网关防病毒功能，但这几项功能并不一定要同时得到使用，不过它们应该是 UTM 设备自身固有的功能。

对于政务网的安全需求是在公网和外网之间实行逻辑隔离,在内网和外网之间实行物理隔离。

网闸其实就是模拟人工数据倒换，利用中间数据倒换区，分时地与内外网连接，但一个时刻只与一个网络连接，保持“物理的分离”，实现数据的倒换。

【答案】C、C。

16.7 网络安全体系

1. 【2010 年题 53 解析】

本题主要考查 ARP 攻击的定义和特点。ARP 攻击是针对以太网地址解析协议（ARP）的一种攻击技术，此种攻击可让攻击者取得局域网上的数据封包甚至可篡改封包，且可让网络上特定计算机或所有计算机无法正常连接。ARP 攻击造成网络无法跨网段通信的原因是伪造网关 ARP 报文使得数据包无法发送到网关。

2. 【2013 年题 36 解析】

重放攻击（Replay Attacks）又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

Kerberos 系统采用的是**时间戳方案来防止重放攻击**，这种方案中，发送的数据包是带时间戳的，服务器可以根据时间戳来判断是否为重放包，以此防止重放攻击。

3. 【2014 年题 42 解析】

1、SQL 注入攻击

SQL 注入攻击是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQL Injection，即 SQL 注入。该种攻击方式与 TCP/IP 漏洞无关。

2、Land 攻击

land 攻击是一种使用相同的源和目的主机和端口发送数据包到某台机器的攻击。结果通常使存在漏洞的机器崩溃。

在 Land 攻击中，一个特别打造的 SYN 包中的源地址和目标地址都被设置成某一个服务器地址，这时将导致接受服务器向它自己的地址发送 SYN 一 ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉。对 Land 攻击反应不同，许多 UNIX 系统将崩溃，而 Windows NT 会变的极其缓慢（大约持续五分钟）。

3、Ping of Death 攻击

在因特网上，ping of death 是一种拒绝服务攻击，方法是由攻击者故意发送大于 65535 字节的 ip 数据包给对方。 TCP/IP 的特征之一是碎裂；它允许单一 IP 包被分为几个更小的数据包。在 1996 年，攻击者开始利用那一个功能，当他们发现一个进入使用碎片包可以将整个 IP 包的大小增加到 ip 协议允许的 65536 比特以上的时候。当许多操作系统收到一个特大号的 ip 包时候，它们不知道该做什么，因此，服务器会被冻结、当机或重新启动。

4、Teardrop 攻击

Teardrop 攻击是一种拒绝服务攻击。是基于 UDP 的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的 IP 包（IP 分片数据包中包括该分片数据包属于哪个数据包以及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。

4. 【2016 年题 39 解析】

在被动攻击(passive attack)中，攻击者的目的只是获取信息，这就意味着攻击者不会篡改信息或危害系统。系统可以不中断其正常运行。

常见的被动攻击包括：窃听和流量分析。

主动攻击(active attack)可能改变信息或危害系统。威胁信息完整性和有效性的攻击就是主动攻击。主动攻击通常易于探测但却难于防范，因为攻击者可以通过多种方法发起攻击。

常见的主动攻击包括：篡改、伪装、重放、拒绝服务攻击。

16.10 其他

1. 【2017 年题 11 解析】

管理距离是指一种路由协议的路由可信度。每一种路由协议按可靠性从高到低，依次分配一个信任等级，这个信任等级就叫管理距离。

正常情况下，管理距离越小，它的优先级就越高，也就是可信度越高。一个管理距离是一个从 0-255 的整数值，0 是最可信赖的，而 255 则意味着不会有业务量通过这个路由。

由此可见，管理距离是与信任相关的，只有选项 C 是相符的。