上海电力大学 2021/2022 学年第二学期期末线上考试

答 题 纸

课号：1601386.01 课程名称：信息安全技术 姓名：＿＿＿＿ 学号：＿＿＿＿

考试时间：2022 年 6 月 20 日 13:30 点— 16:00 点

抄写诚信考试承诺（我郑重承诺：保证严格按照课程考试要求执行考场纪律，由本人独立完成考试，诚信考试。）：我郑重承诺：保证严格按照课程考试要求执行考场纪律，由本人独立完成考试，诚信考试。。本人特此签名：＿＿＿＿

以下为答题区：

一. 填空题

1. 入侵威胁分为：①假冒者 ②保用者 ③秘密用户

2. RBAC考号模型由四个模型组件定义：核心RBAC、①层次RBAC、②静态职责分离 ③动态职责分离。

3. PKI 公钥基础设施是提供①公钥加密和②数字签名 服务的系统或平台，目的是③管理密钥和证书。

4. 保证数据库的完整性是通过①访问控制、②备份的恢复 以及一些③审计的安全机制共同实现

5. 数据加密标准 DES 的密钥长度是①56，子密钥长度是②48，加密轮数是③16。

二. 简答题

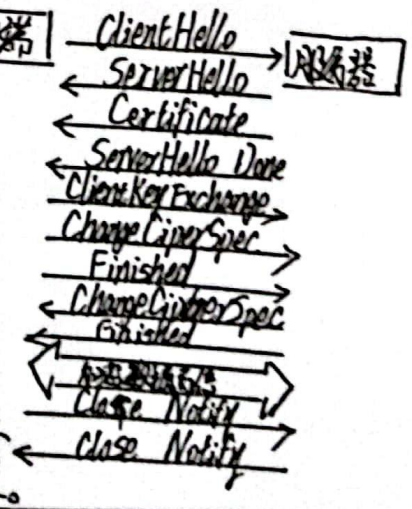
1. 简述采用单向认证的 TLS 握手协议的过程。

一般是在客户端对服务器身份的验证。

1) 客户端向服务器发送 ClientHello 消息，包含客户端提供的密码算法标记、参数以及生成协商中协议需要的随机数

2) 服务器以好、消息响应响应，发送 ServerHello 消息，包括服务器向客户端发送的一个随机数，然后发送 Certificate 消息，包含服务器的公钥证书，再发送 ServerHello Done 消息表示响应完毕。

3) 客户端在收到响应后，对服务器的公钥证书进行验证，通过后，向服务器发送以下3条消息完成握手过程。



上海电力大学 2021/2022 学年第二学期期末线上考试

以下为答题区：

ClientKeyExchange包含服务器公钥加密的一个密钥 ⑤ ChangeCipherSpec表示客户端更改了之前已经协商的算法更改了加密策略. Finished表示完成握手过程 ⑥ 随后服务器也向客户端发送 ChangeCipherSpec 和 Finished 表示确认. 在以上过程结束后，双方进行加密数据传输连接，数据发送完毕后，双方可以发送 Close-Notify 消息结束本次TLS连接.

2. 简要描述主要的身份识别技术.

① 基于口令的身份识别技术：系统为每个授权用户建立一个用户名/口令对，当用户登录系统或使用某项功能时，提示用户输入自己的用户名和口令，系统逐个核对用户名/口令与系统内存有的授权用户的用户名/口令鉴别.

② 基于传统密码的身份识别技术。典型的基于对称密码的双向鉴别协议是Needham-Schroeder协议，该协议要求有可信第三方密钥分发中心(KDC)的参与，采用询问/应答的方式使得通信双方互相识别对方的身份

③ 基于公钥密码的身份识别技术。在无法事先确定共享密钥的情况下，使用Woo-Lam协议通过可信第三方的参与，使得通信双方可以进行有效的身份识别和密钥发放；该技术还可用于通信双方不同时在线的情景，

④ 基于生物特征的身份识别技术，以信息技术为基础，将生物和信息技术交汇渗合为一体. 提取唯一的特征并转换成数字代码，进一步将这些代码组成特征模块；在用户需要进行身份识别时，获取其相应特征并与数据库中的特征模块进行对比进行鉴别.

3. 说明什么是消息鉴别码并简述什么是HMAC

① 消息鉴别码：不对消息进行加密，利用特定的编码方法由消息直接生成才消息鉴别码，把消息鉴别码附加在信息后。接收方可在不解密的情况下获取信息，验证消息的完整性

② HMAC的基本思想是利用基于密钥的Hash函数构造MAC.

4. DBMS中采取的存取管理技术有哪些?

① 用户身份认证技术.

(1) 用户身份验证，系统通过设计好来证实用户身份，进而可以阻止用户非授权用户的访问. 包含操作系统验证，DBMS提供验证和网络安全系统的

以下为答题区：

认证。

(2) 用户身份识别。只有经过数据库授权和验证的用户才是合法的用户，包括授权用户表（包含授权用户的各项信息，完全相符为授权用户）、授权用户权限表（通过该表则赋予用户相应的权利）、禁止使用系统的侵入规则（可以调用数据库的多种规则）自动查询修改技术（防止用户访问数据库中未授权部分。

② 存取控制技术。限制了访问和执行程序可以进行的操作

③ 信息流控制技术。信息流控制机制对系统的所有元素，组成成份等划分类别和级别；负责检查信息的流向，使高保护级别对象不会被传送到低保护级别对象中去。

5. 请简述恶意代码的分类。给出计算机病毒的基本特征。

① 分类：a. 不感染的依附性恶意代码（特洛伊木马、逻辑炸弹、后门或陷门）；b. 不感染的独立型恶意代码（点滴器、繁殖器、恶作剧）；
c. 可感染的依附性恶意代码
d. 可感染的独立性恶意代码（计算机蠕虫、计算机细菌）

② 基本特征：a. 寄生性 b. 传染性 c. 潜伏性 d. 隐蔽性 e. 破坏性 f. 可触发性。

三. 论述题。

1. RSA

(1) 简述 RSA 算法的整体流程。

系统参数建立：实现者寻找两个大素数 p 和 q

密钥生成：计算 $n = pq$，$\varphi(n) = (p-1)(q-1)$

选择随机数 e $(0 < e < \varphi(n))$，满足 $(e, \varphi(n)) = 1$

使用欧几里得算法计算 $d \equiv e^{-1} \pmod{\varphi(n)}$

加密与解密过程：加密：$C \equiv m^e \pmod n$

解密：$m \equiv C^d \pmod n$

(2) 设 $p=13$，$q=7$，$e=7$，$m=10$，计算私钥 d 与密文 C

$n = p \cdot q = 91$

$\varphi(n) = (p-1)(q-1) = (13-1) \times (7-1) = 72$

$d \equiv 7^{-1} \pmod{72} = 31$ 解得

$C \equiv m^d \bmod 91 \equiv 10^{31} \bmod 91$

$\equiv 9^{15} \times 10$

以下为答题区：

2. BLP模型

(1) 什么是BLP模型，其中的强制和自主特征是什么意义

(2) BLP模型有哪些特征，分别有什么优缺点，适用于哪些场景。

(1) BLP模型是一个形式化模型，使用数学语言对系统的安全性质进行描述，BLP模型也是个状态机模型，它反映了多级安全策略的安全特性和状态转换规则。BLP模型定义了系统、系统状态、状态间的转换规则、安全概念，制定了一组安全特性，对系统状态、状态转换规则进行约束

强制：是个有序全序集L，用两个函数f_S和f_O表示主体S和对客体O的强制函数。主体强制函数为 $f_S: S \to L$ $s \mapsto l$

客体的强制函数为 $f_O: O \to L$ $o \mapsto l$

主体的当前强制函数 $f_C: S \to L$ $s \mapsto l$

主体的当前强制是可以变化的，满足 $f_S(s) \geq f_C(s), \forall s \in S$

范畴时 描述了实体对的一种信息，每一个实体被指定到若干范畴内，每个实体又拉到范畴集合的一个子集，而按照包含关系，实体的范畴子集构成一种偏序关系

(2) 特性：①自主安全性 ②简单安全性 ③*一级安全 ④信息流

优点：①是个最早的对多级安全策略进行描述的模型

②是一个严格形式化的模型并给出了形式化的证明

③是个很安全的模型，既有自主访问控制又有强制访问控制

④控制信息只能由低向高流动，满足军事部门等一类对保密性要求特别高的机构需求

缺点：①上级对下级发文受限 ②部门之间横向信息流动被禁止

③缺乏灵活、安全的授权机制 ④存在不安全的地方

适用场景：如军事部门等机密性要求高的场合

四、综合题

1. 即时通信软件

密码技术、身份鉴别技术：通过密码技术进行用户登录，访问QQ或微信服务器

通过UDP等协议建立socket信息交流，实现即时通信

以下为答题区：

IPSEC协议确保通信过程的安全性.

2. VPN技术的作用及如何运用

作用：通过在一个公用网络（如Internet等）中建立一条安全、专用的虚拟通道，连接导地的两个网络，构成逻辑上的虚拟子网。

运作：通过以上海电力大学VPN为例。首先在VPN上通过学号和密码进行登录的技术和身份鉴别技术，再通过隧道技术进行点到点的连接，进而成功访问到校园网.