第七章

7.1 网络安全概述

1.计算机网络的通信面临两大类威胁，即**主动攻击**和**被动攻击。**

2.**被动攻击**是指攻击者从网络上窃听他人的通信内容，通常把这类攻击叫作**截获。**

3.在被动攻击中，攻击者只是观察和分析某一个**协议数据单元PDU**而不干扰信息流，这种被动攻击又叫做**流量分析。**

4.主动攻击有如下几种最常见的方式：

（1）**篡改**

（2）**恶意程序**：有**计算机病毒、计算机蠕虫、逻辑炸弹、后门入侵、流氓软件。**

（3）**拒绝服务Dos**：使一些网站的服务器一直处于“忙”的状态，因而无法向发出请求的客户 提供服务，这种攻击叫作**拒绝服务。**若从互联网上的成百上千个网站集中攻击一个网站，则称为**分布式拒绝服务DDos。**又称为**网络带宽攻击**或**连通性攻击。**

5.一个安全的计算机应设法达到以下四个目标：

（1）**机密性**

（2） **端点鉴别**

（3）**信息的完整性**

（4）**运行的安全性**：**访问控制**对于计算机系统的安全性非常重要。

7.2两类密码体制

1.**对称密钥密码体制**和**公钥密码体制。**

2.所谓对称密码体制，就是**加密密钥和解密密钥都使用相同密钥的密码体制。**

3.**数据加密标准DES**属于对称密钥体制。

4.DES的机密性仅取决于对**密钥的保密**，而**算法**是公开的。

5.在DES之后，有了一种新的加密标准即**高级加密标准AES**（是一种分组密码，有3种加密标准）。

6.公钥密码体制**使用不同的加密密钥和解密密钥。**又称为**非对称密钥密码体制。**

7.公钥密码体制的产生主要有两个方面的原因，一是由于对称密钥密码体制的**密钥分配**问题，二是由于对**数字签名**的需求。

8.若使用高度安全的**密钥分配中心KDC**，会使网络的成本增加。

9.在公钥密码体制中，**加密密钥PK**（即**公钥**）是公开的，而**解密密钥SK**（即**私钥**或**密钥**）是需要保密的。加密算法和解密算法也是公开的。

10.**任何加密算法的安全性取决了密钥的长度，以及攻破密文所需的计算量。**（填空题）

7.3鉴别

1.鉴别的内容有两个：**鉴别发信者**（有实体鉴别、报文鉴别）和**鉴别报文的完整性**（即是否被他人篡改过）。

2.请注意，鉴别与**授权**是不同的概念。

3.**报文鉴别**既鉴别报文的发送者，也鉴别报文的完整性。

数字签名原理

数字签名还有一个功能，就是发送者事后不能抵赖对报文的签名，这叫做**不可否认。**

密码散列函数：

（1）虽然散列函数的输入报文X的长度不受限制，但是计算出的结果H（X）长度应是**较短的**和**固定的。**散列函数H（X）的输出值又叫作**散列值**，或**散列。**

（2）散列函数的输入和输出关系的**多对一**的。会出现不同输入却产生相同输出的**碰撞**现象。因此散列函数应具有较好的**抗碰撞性。**

（3）**MD：报文摘要**

（4）MD5被**安全散列算法SHA**取代。

用报文鉴别码实现报文鉴别：**报文鉴别码MAC，是固定长度的。**

4.实体鉴别：

实体鉴别和报文鉴别不同。报文鉴别是对每一个收到的报文都要鉴别报文的发送者，而实体鉴别是在系统接入的全部持续时间内对和自己通信的对方实体只需验证一次。

（1）**重放攻击**：例如，入侵者C可以从网络上截获A发给B的报文，C**并不需要破译这个报文**（因为破译可能很费时间），而是直接把这个由A加密的报文发给B，使B误以为C就是A，然后B就向伪装成A的C发送许多原本应该发送给A的报文。

（2）对了对付重放攻击，可以使用**不重数。**不重数就是一个**不重复使用的大随机数。**

7.4密钥分配

7.5互联网使用的安全协议

1.IPsec协议族中的协议可以划分为三个部分：

（1）IP安全数据报格式的两个协议：**鉴别首部AH协议**和**封装安全有效载荷ESP协议。**（填空题）

（2）有关加密算法的三个协议。

（3）**互联网密钥交换IKE**（Internet Key Exchange）。

2.使用ESP或AH协议的IP数据报称为**IP安全数据报。**（填空题）

3.IP安全数据报由两个工作方式：**运输方式**和**隧道技术。**（填空题）

4.在发送IP安全数据报之前，在源实体和目的实体之间必须创建一条网络层的逻辑链接，即**安全关联SA。**

5.安全关联是从源点到终点的**单向连接**，它能提供安全服务。

6.安全关联SA的状态信息中的一个32位的连接标识符，称为**安全参数索引SPI。**

7.

7.6防火墙

1.**防火墙**是一种访问控制技术。

2.**防火墙**是一种特殊编程的路由器，安装在一个网点和网络的其余部分之间，目的是实施访问控制策略。

3.一般把防火墙里面的网络称为“**可信的网络”**，把防火墙外面的网络称为“**不可信的网络**”。

4.防火墙技术一般分为两类：**分组过滤路由器**和应用网关（也叫**代理服务器**）。

第九章

1.无线局域网的组成

（1）无线局域网的分类：**有基础设施的**和**无基础设施的。**

（2）802.11是无线以太网的标准，它使用星型拓扑，无线局域网的中心叫作**接入点AP**（也叫作**无线接入点WAP**）。

（3）802.11无线局域网的MAC层使用CSMA/CD协议。

（4）802.11标准规定无线局域网的最小构件是**基本服务集BSS**（Basic Service Set）。

（5）当网络管理员安装AP时，必须为该AP分配一个不超过32字节的**服务集标识符SSID。**

（6）一个基本服务集BSS所覆盖的地理范围叫作一个**基本服务区BSA。**

(7)接入点AP在出厂时就已有了一个唯一的48位二进制数字的MAC地址，其正式名称是**基本服务集标识符BSSID。**

（8）一个服务集可以是孤立的单个服务集，也可通过接入点AP连接到一个**分配系统DS**，然后再连接到另一个基本服务集，这样就构成了一个**扩展服务集ESS。**

（9）ESS也有个标识符，是不超过32字符的字符串**名字**而**不是地址**，叫作扩**展服务集标识符ESSID。**

2.802.11局域网的物理层（书上看着感觉不会考）

3.CSMA/CA

（1）有**隐蔽站问题。**

（2）802.11的MAC层通过**协调功能**，来确定基本服务集BSS中的移动站；它包含两个子层：**分布协调功能DCF**和**点协调功能PCF。**

4.对信道进行预约（RTS、CTS）

（1）为了更好地解决屏蔽站带来的碰撞问题，802.11允许要发送数据的站对信道进行**预约。**

（2）在A站向AP发送数据帧DATA之前，先发送一个很短的控制帧，叫作**请求发送RTS。**

（3）接入点AP若正确收到RTS帧，经过最短的时间间隔SIFS后，就向A站发送一个叫作**允许发送CTS**的控制帧。

5.802.11局域网的MAC：看书

6.其他无线网络