第 4 章 信息安全分析与设计

一、安全基础技术（★★）

1、对称加密

（1）概念

对称加密（又称为私人秘钥加密/共享秘钥加密）：加密与解密使用同一秘钥。

（2）特点

（i）加密强度不高，但效率高

（ii）密钥分发困难。

（大量明文为了保证加密效率一般使用对称加密）

（3）常见对称密钥加密算法

（i）DES：替换+移位、56 位密钥、64 位数据块、速度快、密钥易产生

（ii）3DES(三重 DES)：两个 56 位的密钥 K1、K2

加密：K1 加密->K2 解密->K1 加密

解密：K1 解密->K2 加密->K1 解密 RC-5

（iii）IDEA：128 位密钥、64 位数据块、比 DES 的加密性好、对计算机功能要求相对低，PGP。

（iv）RC-5 算法：RSA 数据安全公司的很多产品都使用了 RC-5。

（v）AES 算法：高级加密标准，又称 Rijndael 加密法，是美国政府采用的一种区块加密标准。

2、非对称加密

（1）概念

非对称加密（又称为公开密钥加密）：密钥必须成对使用（公钥加密，相应的私钥解密）。

（2）特点

加密速度慢，但强度高。

（3）常见非对称密钥加密算法

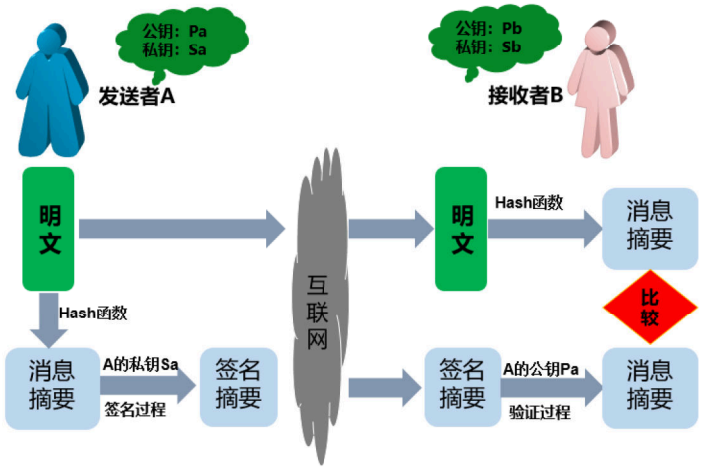
（i）RSA：2048 位（或 1024 位）密钥、计算量极大、难破解

（ii）ECC-椭圆曲线算法

（iii）Elgamal：安全性依赖于计算有限域上离散对数这一难题。

3、信息摘要与数字签名

（1）数字签名的过程如下图所示（发送者使用自己的私钥对摘要签名，接收者利用发送者的公钥对接收到的摘要进行验证）：



（2）常见的摘要算法：MD5(128 位)，SHA(160 位)。

4、数字信封

（i）发送方将原文用对称密钥加密传输，而将对称密钥用接收方公钥加密发送给对方。

（ii）接收方收到电子信封，用自己的私钥解密信封，取出对称密钥解密得原文。

5、PGP

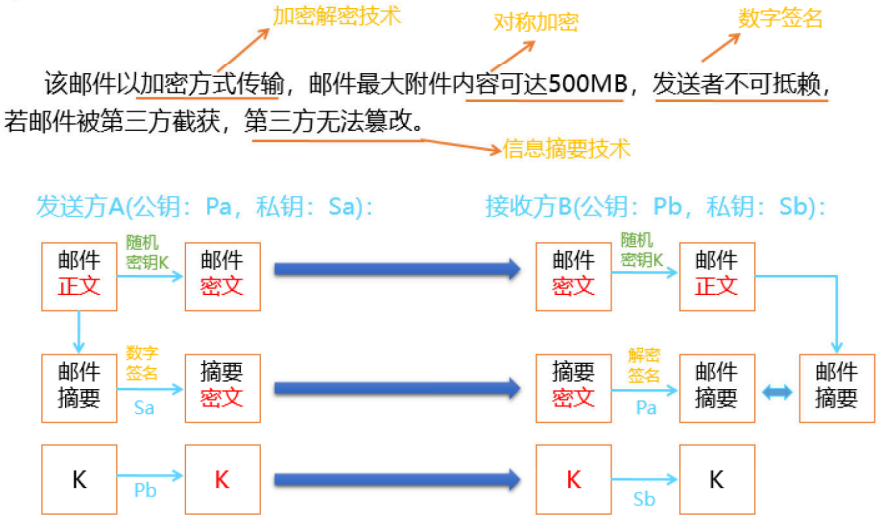
（i）PGP 可用于电子邮件，也可以用于文件存储。采用了杂合算法，包括 IDEA、RSA、MD5、ZIP 数据压缩算法。

（ii）PGP 承认两种不同的证书格式：PGP 证书和 X.509 证书。

（iii） PGP 证书包含 PGP 版本号、证书持有者的公钥、证书持有者的信息、证书拥有者的数字签名、证书的有效期、密钥首选的对称加密算法。

（iv）X.509 证书包含证书版本、证书的序列号、签名算法标识、证书有效期、以下数据：证书发行商名字、证书主体名、主体公钥信息、发布者的数字签名。

5、设计实例



6、PKI 公钥体系

（1）X.509 数字证书内容

证书的版本信息；

证书的序列号，每个证书都有一个唯一的证书序列号；

证书所使用的签名算法；

证书的发行机构名称，命名规则一般采用 X.500 格式；

证书的有效期，现在通用的证书一般采用 UTC 时间格式，它的计时范围为 1950-2049；

证书所有人的名称，命名规则一般采用 X.500 格式；

证书所有人的公开密钥；

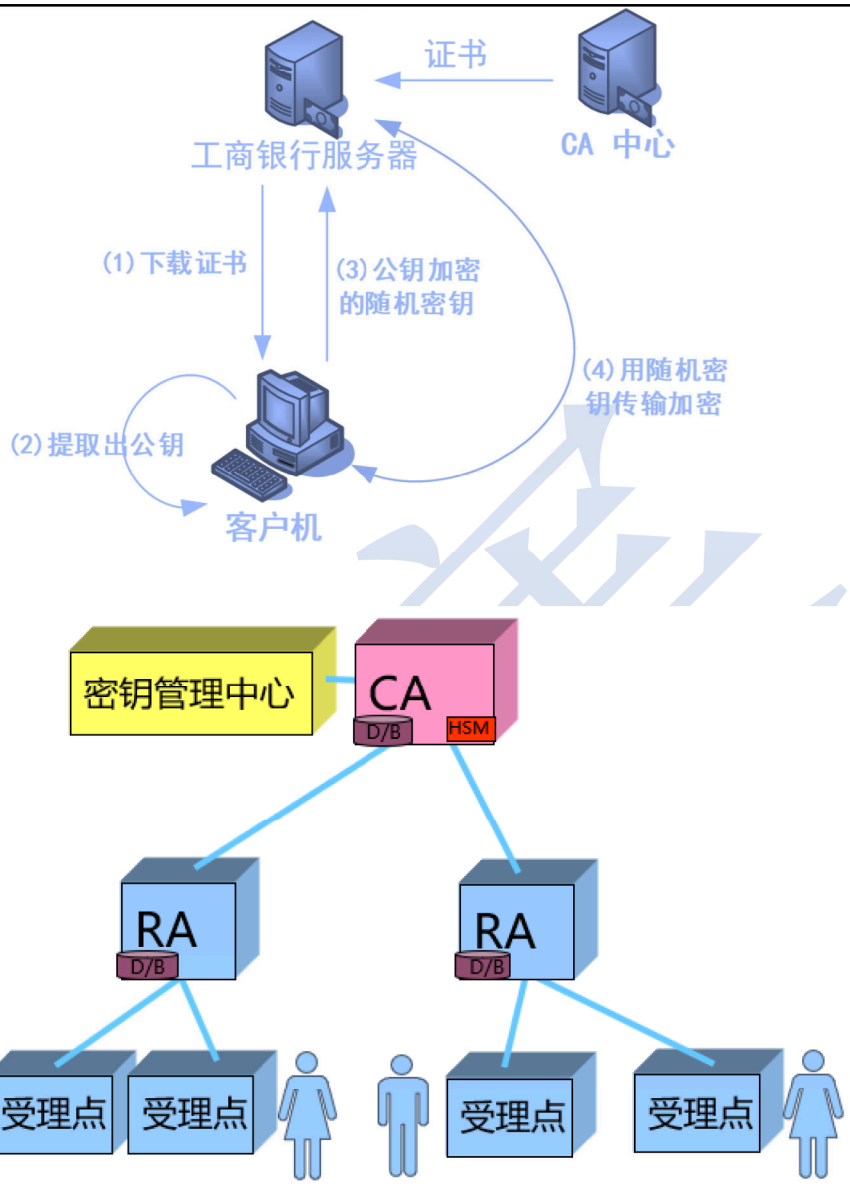
证书发行者对证书的签名。

（2）CA 签名和用户签名的对比

数字证书是由一个权威机构证书授权中心（CA）发行的。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。其中证书授权中心的数字签名是用它自己的私钥完成的，而它的公钥也是公开的，大家可以通过它的公钥来验证该证书是否是某证书授权中心发行的，以达到验证数字证书的真实性。因此要想验证用户 A 数字证书的真伪，需要用 CA 的公钥来完成，

而因为消息 M 是 A 用其私钥加密后的结果，要验证其真实性，就需要用 A 的公钥来解密，如果能解密，说明消息 M 是 A 用其私钥进行了签名的。

（3）公钥体系



CA

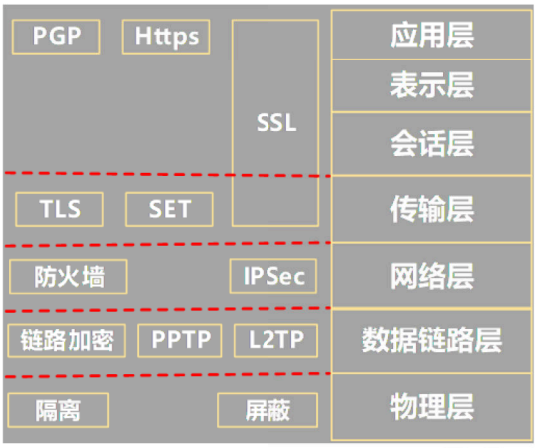
RA

证书受理点

密钥管理中心-KMC

二、网络安全

1、安全协议（★★）



（1）HTTPS 协议是 HTTP 协议与 SSL 协议的结合，默认端口号 443。

（2）PGP：针对邮件的混合加密系统。

（3）SSL：工作在传输层至应用层。

（4）TLS：传输层安全协议。

（5）SET：电子商务。

（6）IPSEC：对 IP 包加密。

2、网络攻击（★★）

（1）分类

（i）被动攻击：收集信息为主，破坏保密性。

攻击类型	攻击名称	描述
被动攻击	窃听（网络监听）	用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息
	业务流分析	通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。
	非法登录	有些资料将这种方式归为被动攻击方式。

（ii）主动攻击：主动攻击的类别主要有：中断（破坏可用性），篡改（破坏完整性），伪造（破坏真实性）

主动攻击	假冒身份	通过欺骗通信系统（或用户）达到非法用户冒充成为合法用户，或者特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒进行攻击。
	抵赖	这是一种来自用户的攻击，比如：否认自己曾经发布过的某条消息、伪造一份对方来信等。
	旁路控制	攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。
	重放攻击	所截获的某次合法的通信数据拷贝，出于非法的目的而被重新发送。
	拒绝服务（DOS）	对信息或其它资源的合法访问被无条件地阻止。

（2）常见的攻击行为

（i）拒绝服务：攻击者利用众多傀儡主机向服务器发送服务请求，导致服务器资源被耗尽，无法提供正常的服务，向其他访问者发送拒绝服务应答。

（ii）重放攻击：攻击者抓取向服务器发送的有效数据包，并利用此数据包不断地向服务器发送，导致服务器一直应答此数据包，从而崩溃。

（iii）业务流分析：通过长期监听被攻击者的数据流，从而分析出相关业务流，可以依此了解被攻击者的一些倾向，常见的广告推送就是建立在业务流分析基础上的。

（3）常见的防御手段（可以结合使用）

（i）防火墙技术：主要了解它的机制是防外不防内，对于 DMZ 非军事区主要放置应用服务器（如邮件服务器，WEB 服务器）。

（ii）漏洞扫描：入侵者可以利用系统漏洞侵入系统，系统管理员可以通过漏洞扫描技术，及时了解系统存在的安全问题，并采取相应措施来提高系统的安全性。

（iii）入侵检测 IDS：基于数据源的分类-审计功能、记录安全性日志。基于检测方法-异常行为检测。

3、安全保护等级

用户自主保护级：适用于普通内联网用户

系统审计保护级：适用于通过内联网或国际网进行商务活动，需要保密的非重要单位

安全标记保护级：适用于地方各级国家机关、金融机构、邮电通信、能源与水源供给部门、交通运输、大型工商与信息技术企业、重点工程建设等单位

结构化保护级：适用于中央级国家机关、广播电视部门、重要物资储备单位、社会应急服务部门、尖端科技企业集团、国家重点科研机构和国防建设等部门

访问验证保护级：适用于国防关键部门和依法需要对计算机信息系统实施特殊隔离的单位

4、安全防范体系

（1）物理环境的安全性。包括通信线路、物理设备和机房的安全等。物理层的安全主要体现在通信线路的可靠性（线路备份、网管软件和传输介质）、软硬件设备的安全性（替换设备、拆卸设备、增加设备）、设备的备份、防灾害能力、防干扰能力、设备的运行环境（温度、湿度、烟尘）和不间断电源保障等。

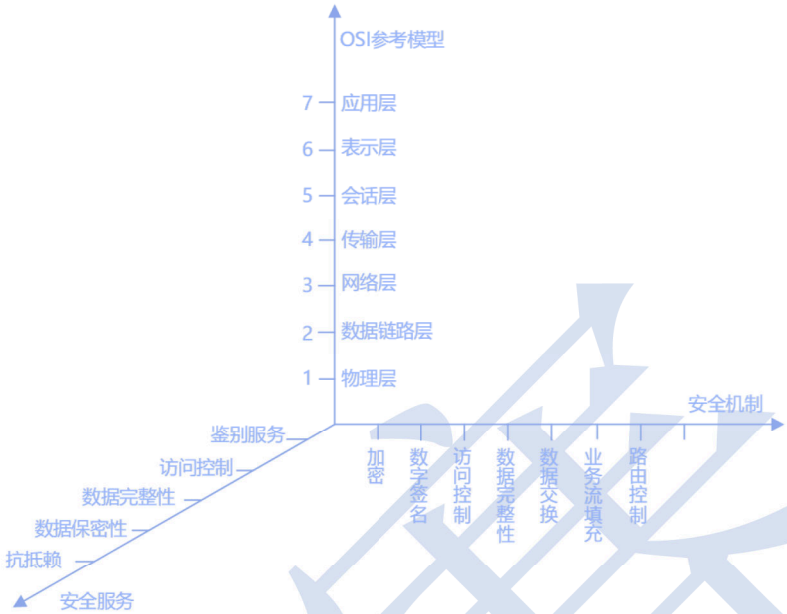
（2）操作系统的安全性。主要表现在三个方面，一是操作系统本身的缺陷带来的不安全因素，主要包括身份认证、访问控制和系统漏洞等；二是对操作系统的安全配置问题；三是病毒对操作系统的威胁。

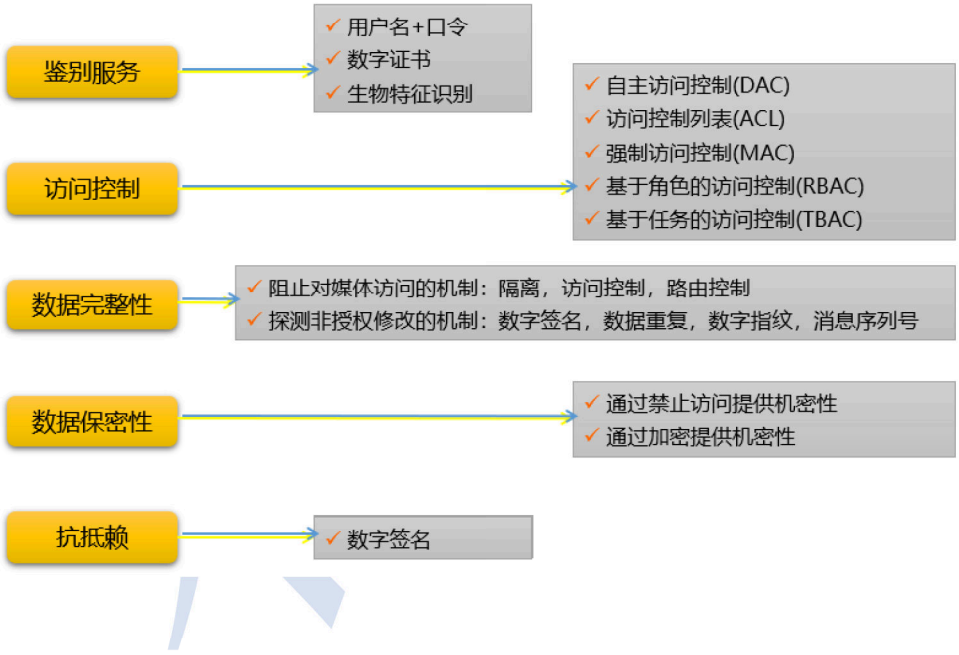
（3）网络的安全性。网络层的安全问题主要体现在计算机网络方面的安全性，包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段和网络设施防病毒等。

（4）应用的安全性。由提供服务所采用的应用软件和数据的安全性产生，包括 Web 服务、电子邮件系统和 DNS 等。此外，还包括病毒对系统的威胁。

（5）管理的安全性。包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个计算机网络的安全，严格的安全管理制度、明确的部门安全职责划分与合理的人员角色配置，都可以在很大程度上降低其他层次的安全漏洞。

5、信息安全体系结构


OSI参考模型
7 应用层
6 表示层
5 会话层
4 传输层
3 网络层
2 数据链路层
1 物理层
安全机制
加密
数字签名
访问控制
数据完整性
数据交换
业务流填充
路由控制
鉴别服务
访问控制
数据完整性
数据保密性
抗抵赖
安全服务


鉴别服务
✓ 用户名+口令
✓ 数字证书
✓ 生物特征识别
访问控制
✓ 自主访问控制(DAC)
✓ 访问控制列表(ACL)
✓ 强制访问控制(MAC)
✓ 基于角色的访问控制(RBAC)
✓ 基于任务的访问控制(TBAC)
数据完整性
✓ 阻止对媒体访问的机制：隔离，访问控制，路由控制
✓ 探测非授权修改的机制：数字签名，数据重复，数字指纹，消息序列号
数据保密性
✓ 通过禁止访问提供机密性
✓ 通过加密提供机密性
抗抵赖
✓ 数字签名