

电子商务概论



第八章 电子商务安全技术

对外经济贸易大学 信息学院

第八章 电子商务安全技术

第一节 电子商务安全基础

第二节 信息安全技术

第三节 网络安全技术

第四节 证书及证书机构



第一节 电子商务安全基础

- 一、电子商务安全威胁
- 二、电子商务安全威胁类别
- 三、产生电子商务安全威胁的原因



一、电子商务安全威胁

- ★ **1999**年信息安全业调查表明，和那些不从事在线商务的公司相比，从事电子商务的公司遭遇黑客非法入侵的可能性高出**57%**。
- ★ 国内统计资料显示，**2000**年，约有**64%**的公司信息系统受到黑客的危害性攻击，其中金融业占总数的**57%**。

二、电子商务安全威胁类别

1. 信息安全
2. 网络（系统）安全
3. 身份确认



三、产生电子商务安全威胁的原因

1. Internet 在安全方面的缺陷

2. 我国电子商务安全威胁的特殊原因



三、产生电子商务安全威胁的原因

1. Internet 在安全方面的缺陷

- ★ **ARPAnet** 是为数据共享设计的，它注重的是开放性、灵活性和方便性。因此，**ARPAnet** 并没有安全方面的考虑。
- ★ **ARPAnet** 从一开始就排除了商业应用，使得 **Internet** 的商业应用在安全上先天不足。



三、产生电子商务安全威胁的原因

1.我国电子商务安全威胁的特殊原因

- ★ 我国的计算机主机、网络交换机、路由器和网络操作系统都来自国外。
- ★ 美国政府对计算机和网络安全技术的出口限制，使得进入我国的电子商务和网络安全产品（包括**Web**浏览器、**Web**服务器、防火墙和路由器等软硬件）均只能提供较短密钥长度的弱加密算法。



第八章 电子商务安全技术

第一节 电子商务安全基础

第二节 信息安全技术

第三节 网络安全技术

第四节 证书及证书机构



第一节 信息安全技术

- 一、信息安全模型与要求
- 二、密码理论
- 三、单钥密码体制
- 四、双钥密码体制
- 五、数字签名
- 六、信息的完整性（哈希函数）
- 七、混合密码系统



一、信息安全模型与要求

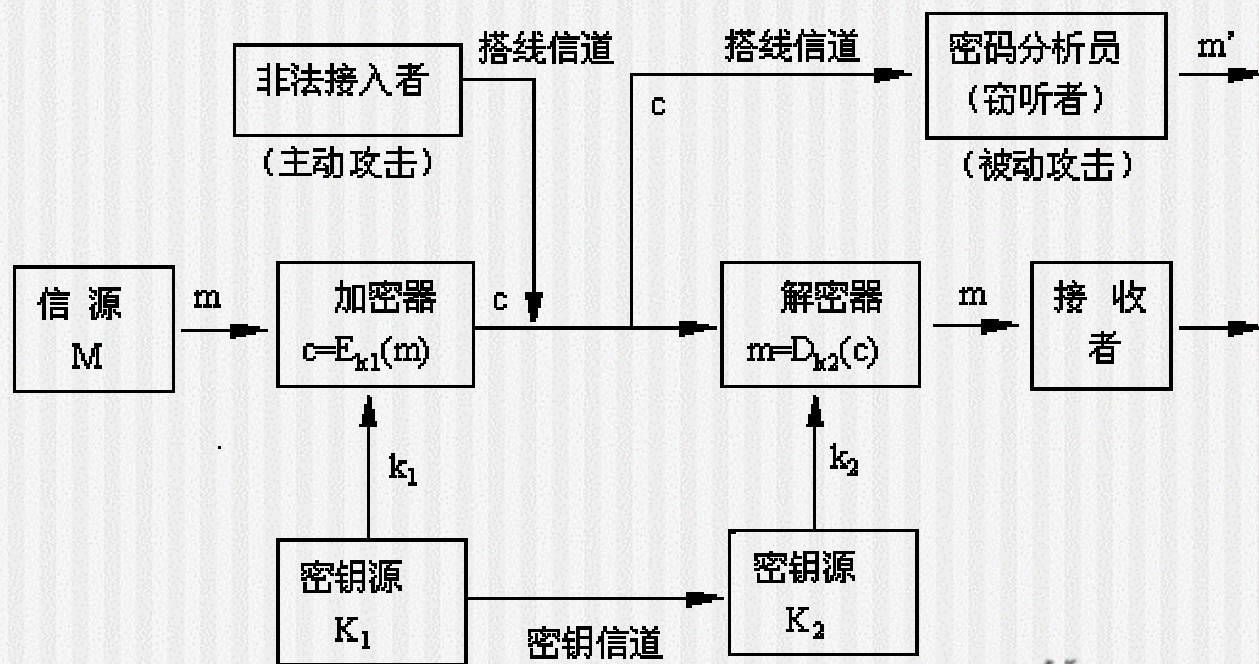
1. 信息安全模型

2. 信息安全要求



一、信息安全模型与要求

1. 信息安全模型



一、信息安全模型与要求

1. 信息安全要求

★ 鉴别性

★ 机密性

★ 有效性

★ 完整性

★ 不可抵赖性



二、密码要求

1. 信息安全要求

- ✦ 使用密码必须能加密也能解密。
- ✦ 密钥和算法必须分开，算法可以公开，保密完全依赖于密钥。



恺撒简单密码体制

1、

密钥=13

算法：字母错位间隔为 13

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

HELLO→URYYB

2、

密钥=12

算法：字母错位间隔为 12

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L

HELLO→TQXXA



对外经济贸易大学

简单二进制密码体制

明文: 1110011010100111

密钥: 1000100001111110

加密算法(E): 本位加(不进位)

解密算法(D): 本位加(不进位)

加密(E):

1110011010100111

1000100001111110

加密结果: 0110111011011001

解密(D):

0110111011011001

1000100001111110

解密结果: 1110011010100111



三、单钥密码体制

1. 典型算法 **DES**
2. 单钥密码体制算法的优缺点
3. 其他单钥密码算法



三、单钥密码体制

1. 典型算法 DES

单钥密码体制也叫对称密钥体制或分组密钥体制。

最著名的保密密钥或对称密钥加密算法 **DES(Data Encryption Standard)** 是由 **IBM** 公司在 **20** 世纪 **70** 年代发展起来的，并经过政府的加密标准筛选后，于 **1976** 年 **11** 月被美国政府采用，**DES** 随后被美国国家标准局和美国国家标准协会 (**American National Standard Institute, ANSI**) 承认。



三、单钥密码体制

1. 典型算法 DES

DES使用**56**位密钥对以位的数据块进行加密，并对**64**位的数据块进行**16**轮编码。与每轮编码时，一个**48**位的“每轮”密钥值由**56**位的完整密钥得出来。**DES**用软件进行解码需要用很长时间，而用硬件解码速度非常快，但幸运的是当时大多数黑客并没有足够的设备制造出这种硬件设备。在**1977**年，人们估计要耗资两千万美元才能建成一个专门计算机用于**DES**的解密，而且需要**12**个小时的破解才能得到结果。所以，当时**DES**被认为是一种十分强壮的加密方法。



三、单钥密码体制

DES算法的应用

A(发送方)明文 M

$$C = E_{K_{DES}}(M)$$

B (接收方)

$$M = D_{K_{DES}}(C)$$



三、单钥密码体制

2. 单钥密码体制算法的优缺点

- ★ 加解密速度快，可用来处理大批量数据
- ★ 不适合密钥分配和管理



三、单钥密码体制

3. 其他单钥密码算法

- ✦ **IDEA, RC-5, SAFER K-64**
- ✦ **LUCIFER, FEAL-N, LOKI-89, CAST**
- ✦ **SKIPJACK, MADRYGA, REDOC**
- ✦ **REDOCI II, KHUFU, KHAFRE等**
等。



四、双钥密码体制

- 典型算法 **RSA**
- 2. 双钥密码体制算法的优缺点
- 3. 其他双钥密码算法



四、双钥密码体制

1. 典型算法 **RSA**

双钥密码体制也叫非对称密钥体制或公开密钥体制。

1978年就出现了**RSA**算法，它是第一个既能用于数据加密也能用于数字签名的算法。它易于理解和操作，也很流行。算法的名字以发明者的名字 (**Ron Rivest, Adi Shamir**和 **Leonard Adleman**)命名。但**RSA**的安全性一直未能得到理论上的证明。



四、双钥密码体制

1. 典型算法 RSA

RSA的安全性依赖于大数分解。公钥和私钥都是两个大素数(大于**100**个十进制位)的函数。据猜测,从一个密钥和密文推断出明文的难度等同于分解两个大素数的积。



四、双钥密码体制

1. 典型算法 RSA

★ 密钥对的产生

选择两个大素数； p 和 q 。计算；

$$n = p q$$

然后随机选择加密密钥 e ；要求 e 和

$(p-1)(q-1)$ 互质。最后，利用 **Euclid** 算法计算解密密钥 d ，满足

$$ed = 1 \pmod{(p-1)(q-1)}$$

其中 n 和 d 也要互质。数 e 和 n 是公钥， d 是私钥。两个素数 p 和 q 不再需要，应该丢弃，不要让任何人知道。



四、双钥密码体制

1. 典型算法 RSA

★ RSA 算法的应用

加密信息 m (二进制表示) 时, 首先把 m 分成等长数据块 m_1, m_2, \dots, m_i , 块长 s , 其中 $2^s \leq n$, s 尽可能的大。对应的密文是:

$$c_i = m_i^e \pmod{n}$$

解密时作如下计算:

$$m_i = c_i^d \pmod{n}$$



四、双钥密码体制

A(发送方)明文 M

B (接收方)

$$C = E_{K_{PB}}(M)$$

$$M = D_{K_{SB}}(C)$$



四、双钥密码体制

2. 双钥密码体制算法的优缺点

- ✦ 适合密钥分配和管理
- ✦ 算法速度慢，只适合加密小数量的信息



四、双钥密码体制

3. 其他双钥密码算法

- ★ **ElGamal (1984, 1985)**
- ★ **椭圆曲线 ECDLC, ECC**



五、数字签名

A(发送方, 明文 M)

B (接收方)

$$C = E_{K_{SA}}(M)$$

$$M = D_{K_{PA}}(C)$$



六、信息的完整性（哈希函数）

哈希函数也叫杂凑函数。利用哈希函数产生定长（**128**位）的样本，叫哈希函数值（杂凑函数值），有些书上叫消息摘要。不同的文件其哈希函数值是不同的。因此，哈希函数值能反映出原文件经传递后的真伪。



六、信息的完整性（哈希函数）

A(发送方, 明文 M)

B (接收方)

计算 M 的 h 值 $h = H(M)$

将 M, h 发给 B

计算收到的 M 的 h 值 $h' = H(M)$

比较 h 和 h'



七、混合密码系统

- 混合密码系统的功能

2. 混合密码系统的组成



七、混合密码系统

1. 混合密码系统的功能

- ✦ 对信息能加解密
- ✦ 有信息完整性检验
- ✦ 有发送不可否认
- ✦ 实现加解密“一次一密”
- ✦ 充分发挥单、双密钥机制的优点



七、混合密码系统

2. 混合密码系统的组成

A (发送方, 明文 M)

- 1、 $h = H(M)$
- 2、 $h_1 = E_{KSA}(h)$
- 3、 $M' = M + h_1$
- 4、 随机产生一个 K_{DES}
- 5、 $C_1 = E_{KPB}(K_{DES})$
- 6、 $C_2 = E_{KDES}(M')$

发送给B

B (接收方)

- 1、 $K_{DES} = D_{KSB}(C_1)$
- 2、 $M' = D_{KDES}(C_2)$
- 3、 从 M' 中分离出 M_1, h_{11}
- 4、 $h' = D_{KPA}(h_{11})$
- 5、 $h_2 = H(M_1)$
- 6、 检验 h_2 是否等于 h'

若 $h_2 = h'$ 则 $M_1 = M$,

若 $h_2 \neq h'$ 则 $M_1 \neq M$.



第八章 电子商务安全技术

第一节 电子商务安全基础

第二节 信息安全技术

第三节 网络安全技术

第四节 证书及证书机构



第三节 网络安全技术

- 一、网络安全需求
- 二、接入控制
- 三、防火墙
- 四、代理服务器



一、网络安全需求

1. 认证性
2. 完整性
3. 保密性
4. 接入控制
5. 密钥管理
6. 传输控制



二、接入控制

1. 接入控制的作用
2. 接入控制的功能
3. 接入控制的策略
4. 接入控制的方式



二、接入控制

- 接入控制的作用

接入控制是保证网络安全的重要手段。它通过一组机制控制不同级别的主体对目标资源的不同授权访问，在对主体认证之后实施网络资源安全管理和使用。



二、接入控制

2. 接入控制的功能

- ✦ 阻止非法用户进入系统;
- ✦ 允许合法用户进入系统;
- ✦ 使合法用户按其权限进行各种信息活动。



二、接入控制

3. 接入控制的策略

- ★ 最小权益策略：按主体执行任务所需权力最小化分配权力。
- ★ 最小泄露策略：按主体执行任务所知道的信息最小化分配权力。
- ★ 多级安全策略：主体和客体按普通、秘密、机密、绝密级划分，进行权限和流向控制。



二、接入控制

4. 接入控制的方式

- ★ 自主式接入控制 **DAC**: 由资源拥有者分配接入权。
- ★ 强制式接入控制 **MAC**: 由系统管理员来分配接入权限和实施控制。



三、防火墙

1. 防火墙设计需要满足的基本原则
2. 防火墙的组成
3. 防火墙的分类
4. 防火墙的安全业务



三、防火墙

1. 防火墙设计需要满足的基本原则

- ✦ 由内到外和由外到内的业务流必须经过防火墙
- ✦ 只允许本地安全政策认可的业务流通过防火墙
- ✦ 尽可能控制外部用户访问内域网，应严格限制外部用户进入内域网
- ✦ 具有足够的透明性，保证正常业务的流通
- ✦ 具有抗穿透攻击能力、强化记录、审计和告警

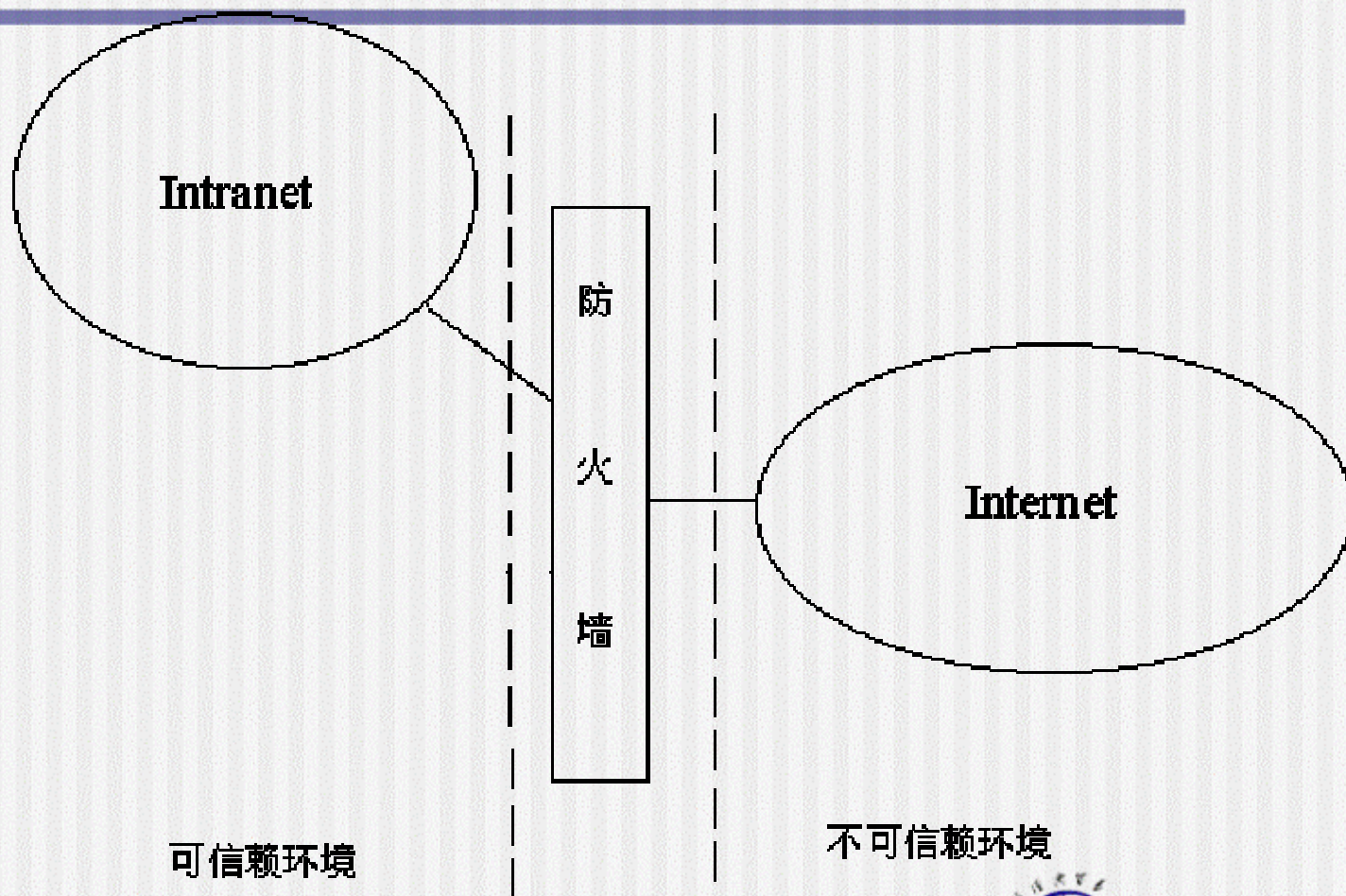
三、防火墙

2. 防火墙设计需要满足的基本原则

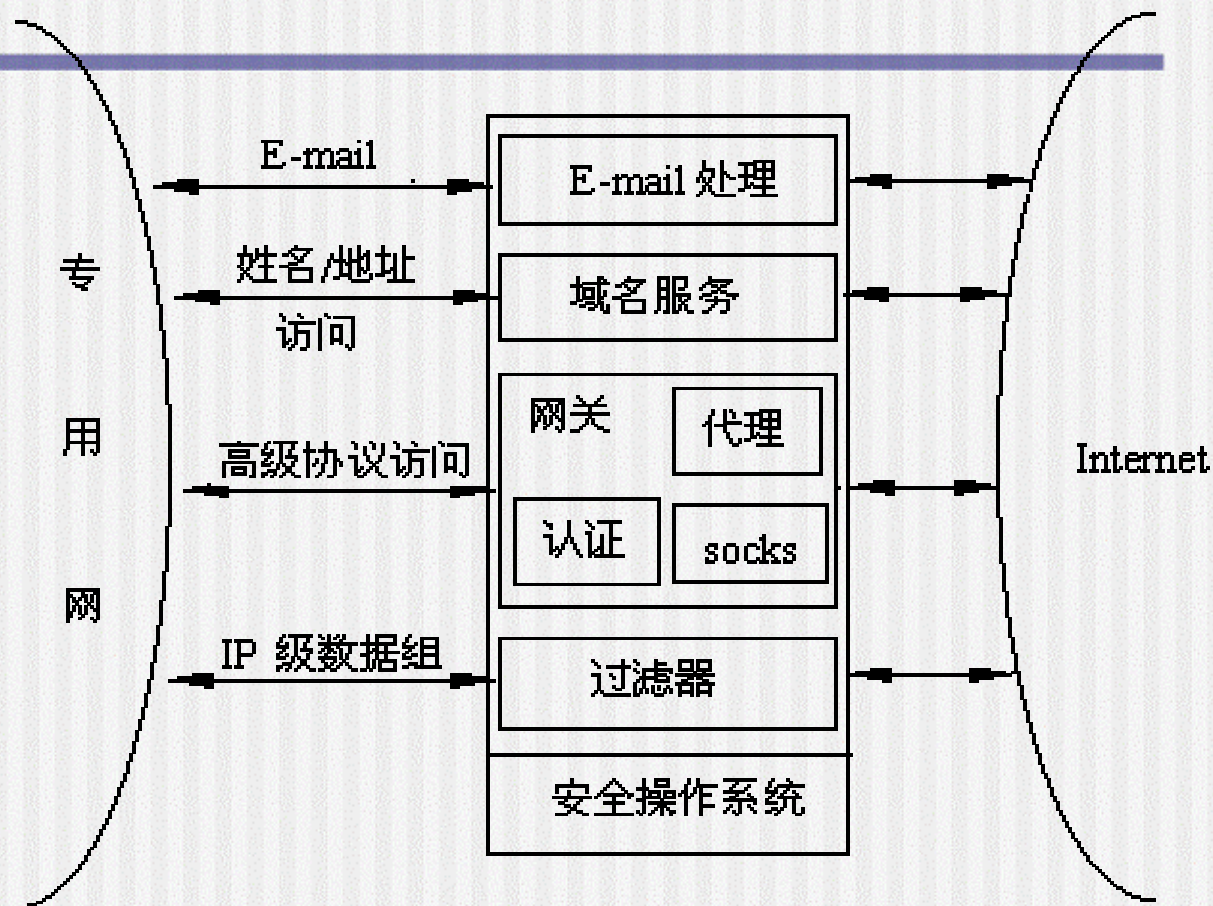
防火墙主要包括安全操作系统、过滤器、网关、域名服务和 **E-mail** 处理。



三、防火墙



三、防火墙



防火墙

三、防火墙

3. 防火墙的分类

- ✦ 分组过滤网关
- ✦ 应用级网关
- ✦ 线路级网关



三、防火墙

4. 防火墙的安全业务

- ✦ 用户认证
- ✦ 域名服务
- ✦ 邮件处理
- ✦ **IP**的安全性
- ✦ 防火墙的**IP**的安全性



四、代理服务器

- ★ 代理服务器在 **TCP/IP** 应用层上可干预并检验数据流。
- ★ 每一类应用都要有一个单独的代理服务器。



五、计算机病毒的防治

1. 计算机病毒的本质
2. 计算机病毒的危害
3. 企业网络防病毒方法



五、计算机病毒的防治

1. 计算机病毒的本质

计算机病毒的本质也是一种计算机程序，这种程序只会对计算机和网络带来危害。



五、计算机病毒的防治

2. 计算机病毒的危害

- ✦ 病毒自我复制，大量占据内存，造成计算机死机
- ✦ 病毒破坏文件，造成重要数据丢失
- ✦ 病毒利用邮件系统大量复制、传播，造成网络阻塞，甚至瘫痪。
- ✦ 有的病毒造成计算机内储存的机密信息被窃取；甚至还有有的计算机信息系统和网络被人控制。



五、计算机病毒的防治

3. 企业网络防病毒方法

- ✦ 不要随便使用在别的机器上使用过的可擦写存储介质（如：软盘、硬盘、可擦写光盘等）。
- ✦ 坚持定期对计算机系统进行计算机病毒检测。
- ✦ 坚持定期对计算机系统进行计算机病毒检测。
- ✦ 严禁玩电子游戏。
- ✦ 不要使用盗版光盘上软件。
- ✦ 接入**Internet**的用户,不要轻易下载使用免费的软件。
- ✦ 不要轻易打开不明来路的电子邮件及其附件。



六、计算机及网络系统安全策略

1. 计算机及网络系统安全策略的必要性
2. 计算机及网络系统安全策略的主要内容



六、计算机及网络系统安全策略

1. 计算机及网络系统安全策略的必要性

任何安全措施都要人来执行，要有严格的规章制度来保证。无论多么先进的安全技术，如果没有人的配合，仍然达不到安全的效果。



六、计算机及网络系统安全策略

2. 计算机及网络系统安全策略的主要内容

- ✦ 计算机网络系统建设的安全考虑
- ✦ 计算机网络系统应用的规章制度
- ✦ 严格的审计
- ✦ 经常进行员工安全知识的培训和规章制度执行情况的检查



第八章 电子商务安全技术

第一节 电子商务安全基础

第二节 信息安全技术

第三节 网络安全技术

第四节 证书及证书机构



第四节 证书及证书机构

- 一、身份证明的需求
- 二、身份证明系统的组成和要求
- 三、公钥证书
- 四、公钥证书的吊销
- 五、证书机构



一、身份证明的需求

- ✦ 现实生活中，身份欺诈是不可避免的。
- ✦ 网络环境中的交易是不谋面的，身份证实更显重要。



二、身份证明系统的组成和要求

1. 身份证明系统的组成
2. 身份证明系统的要求



二、身份证明系统的组成和要求

1. 身份证明系统的组成

- ✦ 一般一个身份证明系统由三方组成，一方是出示证件的人，称作示证者，又称申请者，提出某种要求；第二方为验证者，检验示证者提出的证件的正确性和合法性，决定是否满足其要求；第三方是攻击者，可以窃听和伪装示证者骗取验证者的信任。
- ✦ 认证系统在必要时会有第四方，即可信赖方参与，用以调解纠纷。



二、身份证明系统的组成和要求

2. 身份证明系统的要求

- ✦ 验证者正确识别合法示证者的概率极大化。
- ✦ 不具可传递性，验证者不能用示证者提供的信息，伪装示证者骗取其他人的信任。
- ✦ 攻击者伪装示证者欺骗验证者成功的概率小到可以忽略
- ✦ 计算有效性，计算量要小。
- ✦ 通信有效性，为实现身份证明所需通信次数和数据量要小
- ✦ 秘密参数安全存储。



三、公钥证书

1. 公钥证书基本格式
2. 公钥证书的发行与分配
3. 证书的使用期



三、公钥证书

1. 公钥证书基本格式

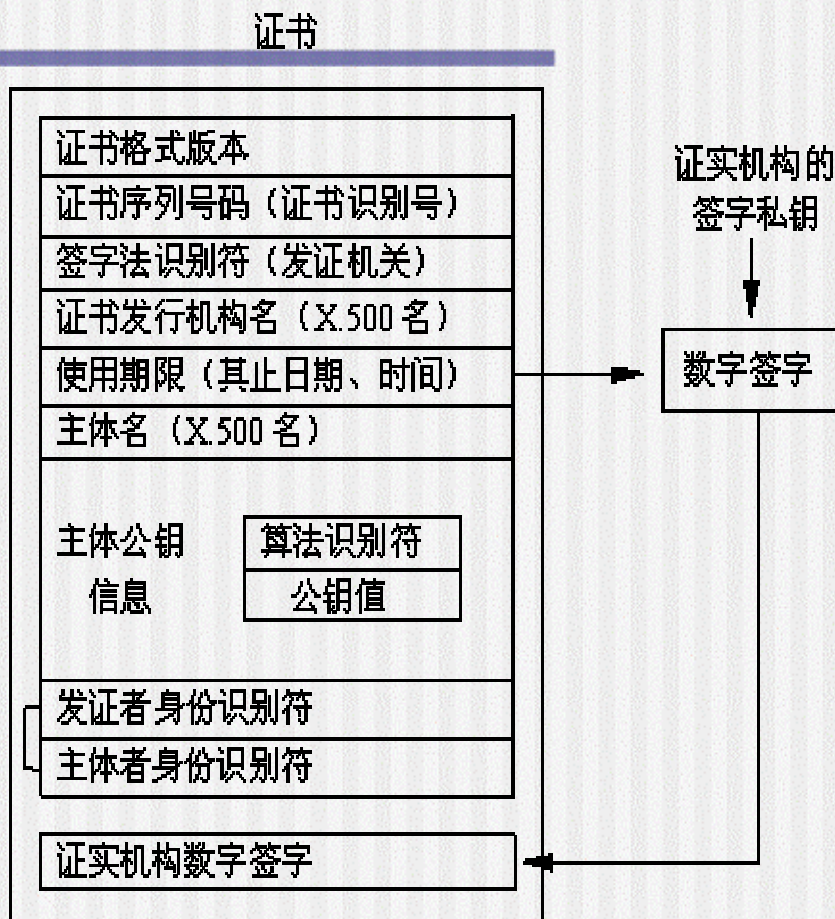
- ★ **X.509 Ver.1和Ver.2** 的基本格式
- ★ **X.500** 的命名树构造



三、公钥证书

1. 公钥证书基本格式

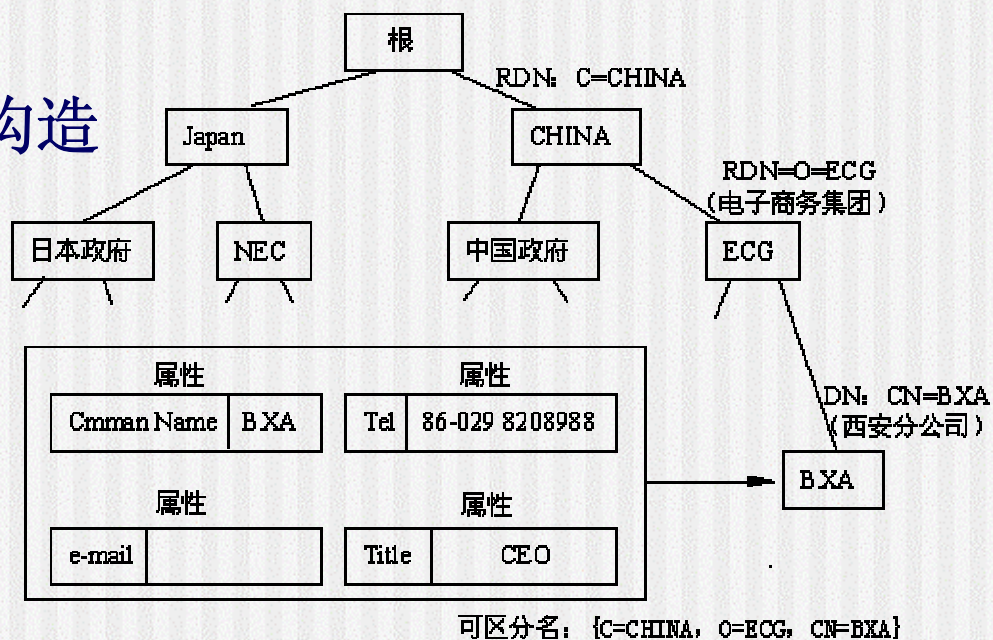
- ★ X.509 Ver.1和 Ver.2 的基本格式



三、公钥证书

1. 公钥证书基本格式

★ X.500 的命名树构造



三、公钥证书

2. 公钥证书的发行与分配

- ★ 证书申请
- ★ 主体认证
- ★ 证书生成
- ★ 证书更新
- ★ 证书分配



三、公钥证书

3. 证书的使用期

- ✦ 证书的使用期视用途不同有所不同。
- ✦ 用于加密的证书由于使用频繁，为安全其使用期较短。
- ✦ 用于签字的证书则使用期较长。



三、公钥证书

4. 公钥证书的吊销

- ✦ 申请吊销
- ✦ 证书吊销表 (Certificate Revocation List)
- ✦ 广播吊销表
- ✦ 立即吊销



三、公钥证书

5. 证书机构

- ★ 证书机构是可信赖机构
- ★ 证书机构用于创建和发布证书，它为一个称为安全域的有限群体发放证书
- ★ 证书机构负责维护和发布吊销表
- ★ 证书机构间建立可信赖的公钥证书证实链路----通用层次结构



证实链

