第8章　电子商务安全

- 电子商务系统安全问题概述
- 电子商务系统安全技术
- 电子商务安全交易协议
- 电子商务系统的运行管理安全

电子商务中的安全问题

- 什么是电子商务中的安全问题
- 电子商务安全的重要性
- 电子商务安全的层次分类与表现形式
- 常见的安全威胁

什么是电子商务系统安全

- 就是保护与电子商务交易相关的各类系统资源的安全,保证电子商务系统的正确运行

案例: CDNow公司受到的攻击

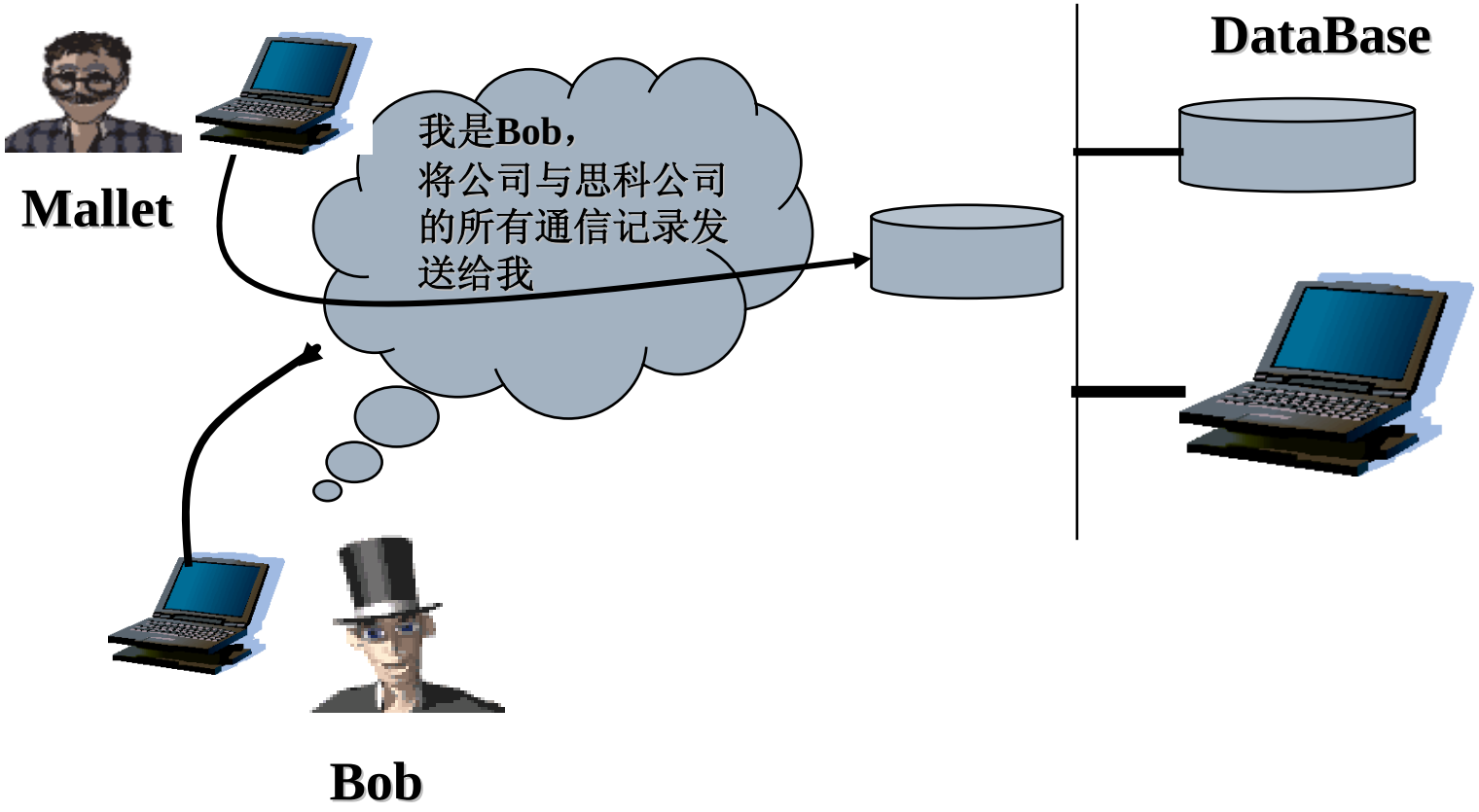
- CDNow是美国一家从事音像制品电子零售的电子商务企业。2000年1月，俄罗斯的一个叫做Maxum的黑客从该公司的网站上偷取了30万条信用卡记录，并向该公司敲诈10万美元。当CDNow公司拒绝其要求时，黑客开始逐条公布信用卡记录的内容。在这种情况下，当时美国运通公司（American Express）不得不暂时停止给该公司用户发行新卡。

网上信息的窃听与数据的窃取

登录：**foo.bar.org**
用户名：**dan**
密码：

M-y-p-a-s-s-w-o-r-d d-a-n

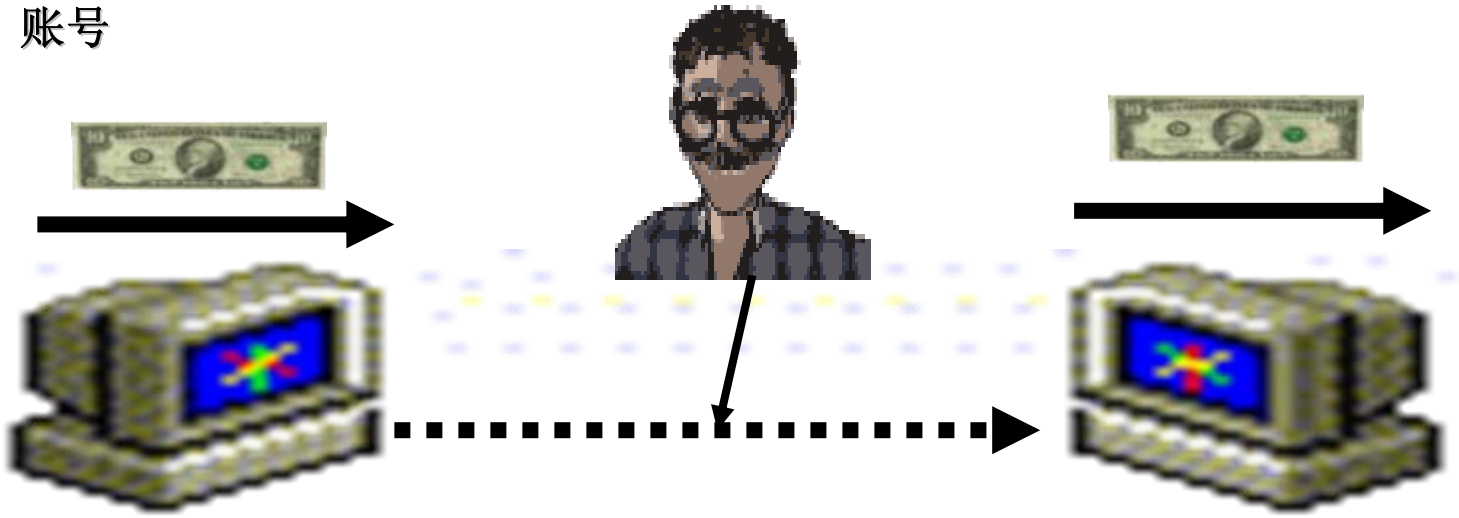
对用户身份的仿冒



数据篡改

存1000美元到Bob的账号

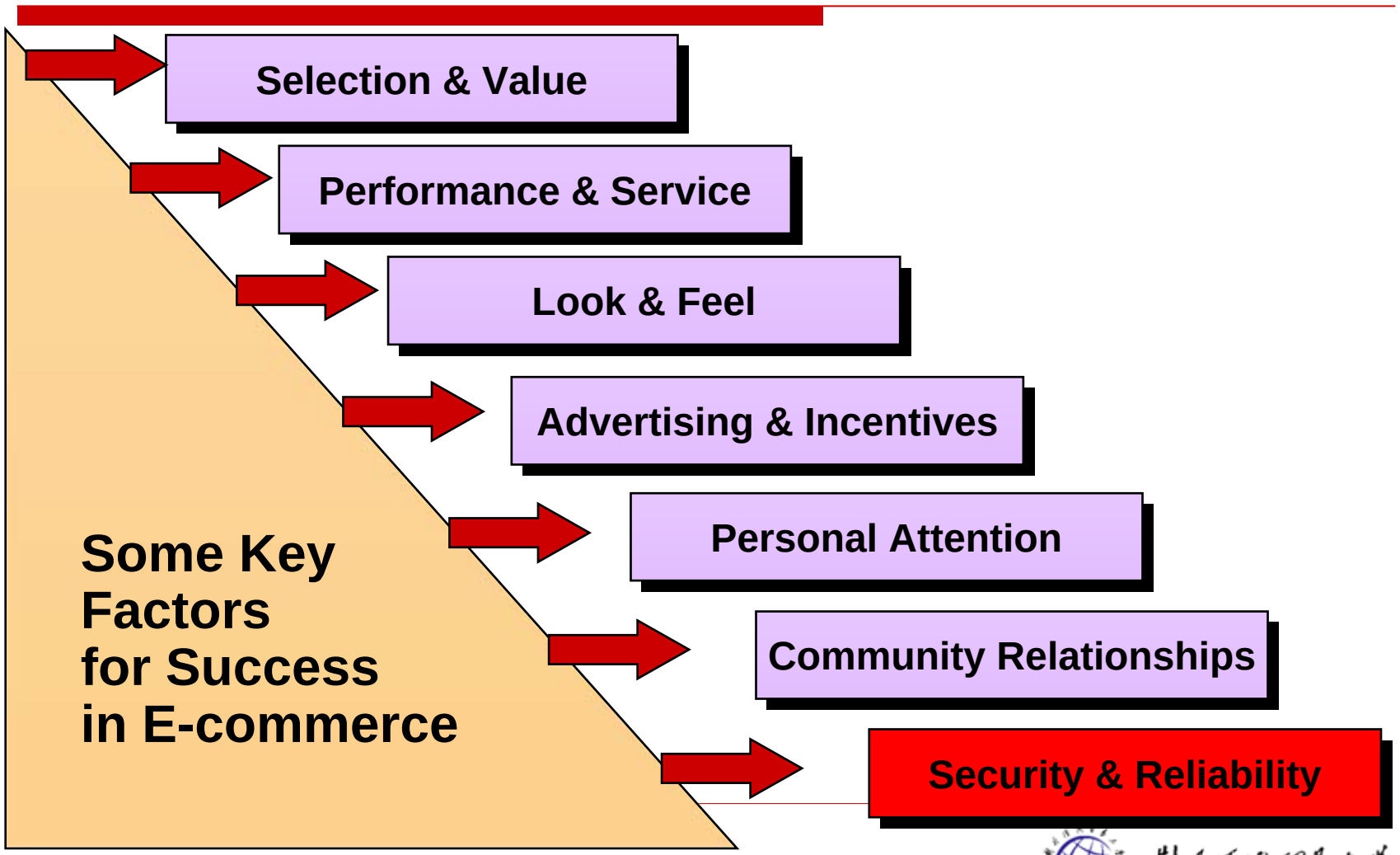
存900美元到Mallet的账号
存100美元到Bob账号



客户

银行

电子商务中安全的重要性



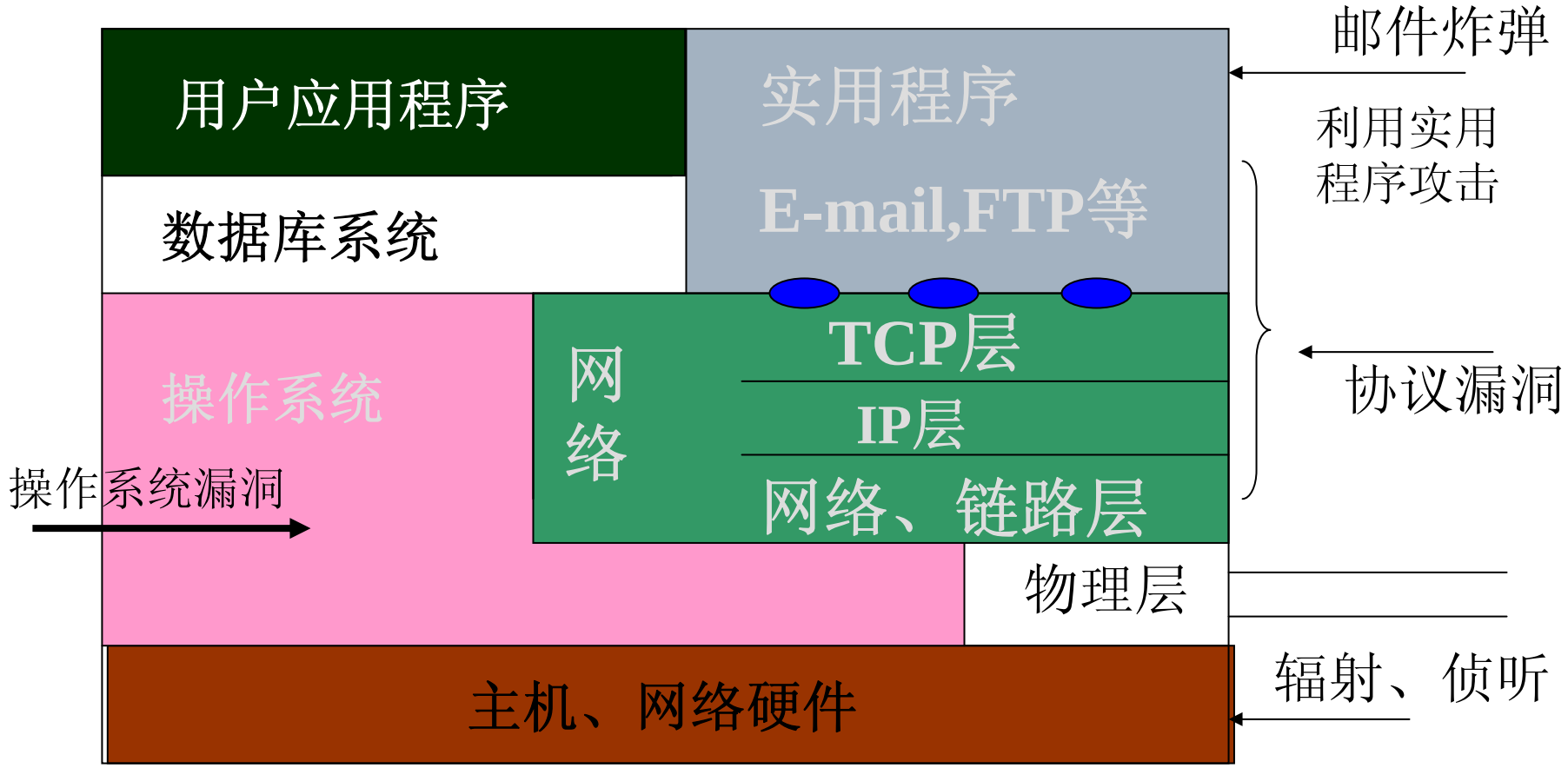
电子商务中安全的重要性

- 安全技术实现电子交易过程的程序合法性
- 关系到消费者、企业、银行、电子商务网站或服务机构等多方的切身利益
- 直接影响电子商务的自身发展
- 关系到国家的安全和社会的稳定

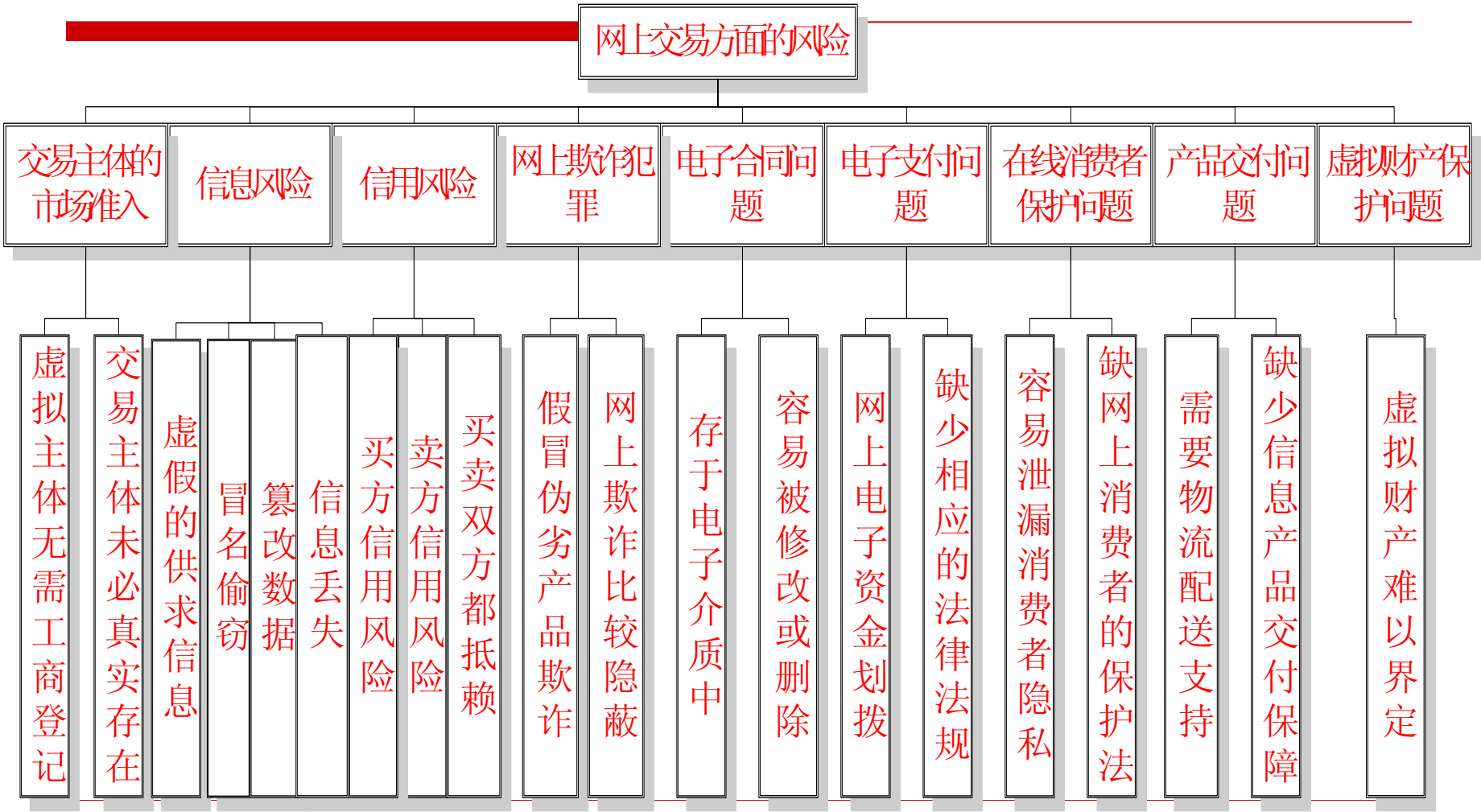
电子商务中的风险分类

- 计算机网络与系统方面的风险
- 网上交易方面的风险
- 管理方面的风险
- 政策法律方面的风险

计算机网络与系统方面的风险



网上交易方面的风险



电子商务交易安全威胁的表现形式

- 对电子商务系统
  - 窃取商务信息
  - 篡改商务信息
  - 假冒用户身份
  - 否认所做操作
  - 重发信息

电子商务交易安全威胁的表现形式

- 对商家经常面临的安全问题有：

① 电子商务中心系统的安全性被破坏。
② 竞争者的威胁。
③ 假冒的威胁。
④ 信用的威胁。

电子商务交易安全威胁的表现形式

- 消费者经常面临的安全问题有：

① 虚假订单。
② 付款后收不到商品。
③ 机密性丧失。
④ 拒绝服务。

管理方面的风险

- 管理制度合理及完备程度
- 制度执行的力度
- 人员的意识、素质和技能
- 辅助管理的技术手段不完善
- 管理的复杂性

政策法律方面的风险

- 法律滞后带来的风险
- 对法律的认识不足带来的风险
- 在电子商务系统中技术手段对相关法律要求体现不充分带来的风险

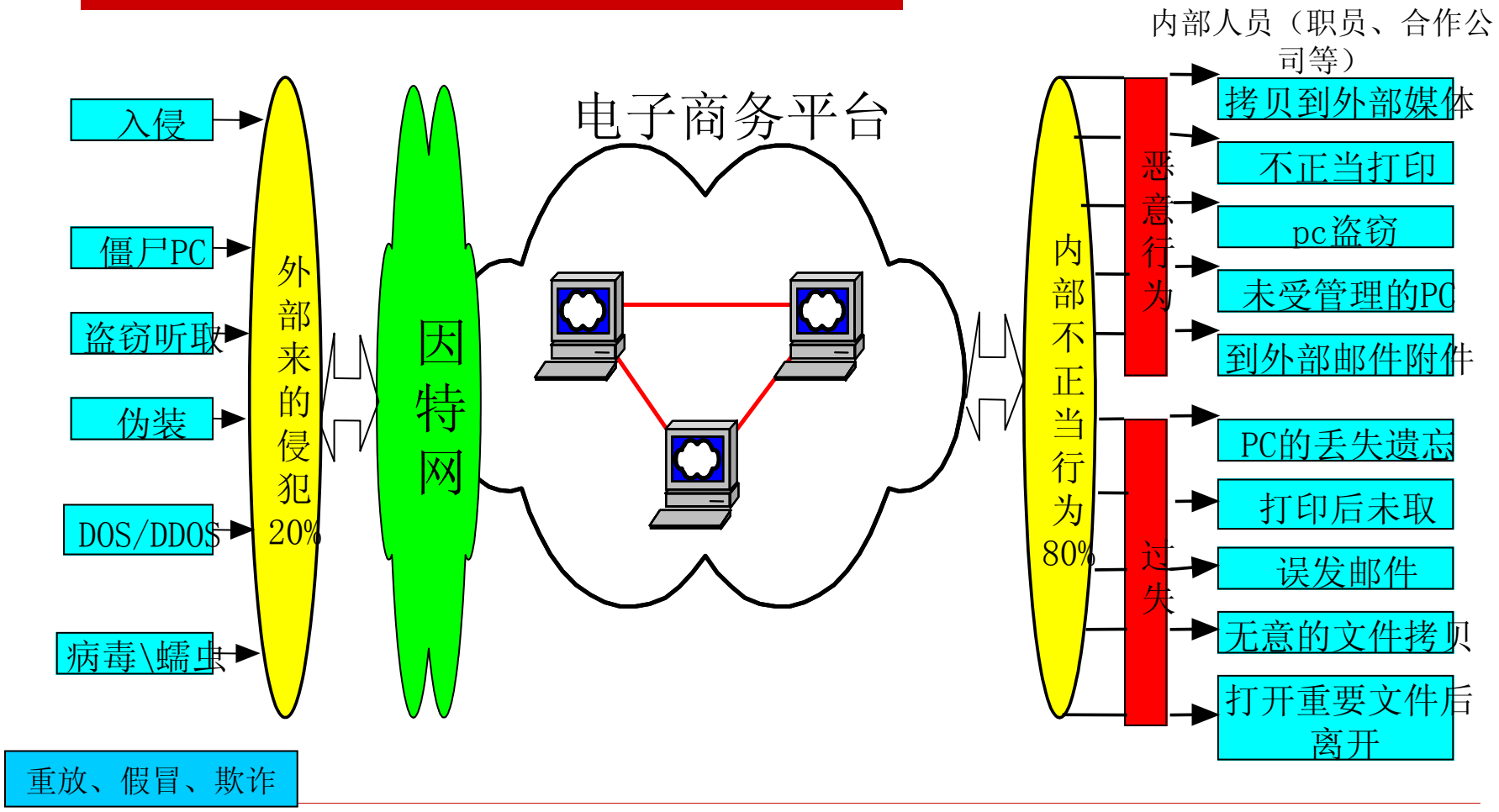
安全性事件造成的后果

公司	件数	泄露原因	被害规模
京都府 宇治市	22万	犯人：信息处理承包公司职员 方法：不正当带出/复制到光盘 原因：访问权限/客户信息管理不善	3名被害居民起诉 京都地裁判决： 赔偿金4万5千日元 （1万5千日元/人）
宽带网络 大型 公司Y	460万	犯人：销售代理经营者 （可能内部有帮手） 方法：不正当带出/复制到外部媒体 （CD-R等） 原因：访问权限/客户信息管理不善	460万被害人 给每人赔偿500日元代金券(总额：约40亿) 发生了恐吓未遂事件
度假村- O公司	12.1万	犯人：内部以及外部委托人员（可能） 方法：客户信息的不正当带出(可能) 日志收集不足，无法确定 原因：访问权限/客户信息管理不善	被害者12万1000人给每人赔偿500日元代金券
信用卡记账事务处理公司-C公司	4000万以上	犯人：外部或内部人员（可能） 方法：通过非法程序取出数据 原因：对非法程序的监视不够	卡号、有效期、姓名等的信用卡信息大量流失

安全性事件造成的后果

公司	泄密内容	泄密原因	被害等
广州好又多百货商业有限公司	5年内的供货商名址、商品购销价格、公司经营业绩及会员客户名单	犯人：公司咨询部管理人员 方法：FTP下载/光碟拷贝/打印 原因：访问权限/信息管理不善	约合4200万元人民币的损失
航空工业总公司某研究所	国防重点工程详细资料	犯人：内部研究人员 方法：非法带出/在家上网 原因：离网管理/信息管理不善	造成重大泄密，有期徒刑8个月
某大型企业研发中心	新产品开发资料	犯人：内部人员（可能性） 方法：科研情报非法带出（可能性） 记录不足、无法确定犯人 原因：访问权限/信息管理不善	约合1200万元人民币的损失
电信方案提供商亚信	给电信运营商的解决方案和技术文档	犯人：内部人员（可能性） 方法：科研情报非法带出（可能性） 记录不足、无法确定犯人 原因：访问权限/信息管理不善	企业信誉度下降
武汉某生物制药公司	新药技术资料	犯人：内部员工 方法：光碟拷贝/非法带出 原因：访问权限/信息管理不善	约合1200万元人民币的损失，有期徒刑1年半

电子商务面临的威胁形式



常见的电子商务安全威胁

- 自然灾害
- 环境因素
- 软硬件质量及其安全漏洞
- 误操作
- 病毒
- 黑客
- 欺诈和盗窃

电子商务面临的安全威胁

- 分类：自然威胁和人为威胁
  - 人为威胁的三个级别
    - C级威胁。个体信息犯罪，也就是信息攻击者是个体，单点攻击，采用一些简单的攻击工具。虽然这种攻击可以逐步实施自动化，但是攻击是单一的，破坏有限。
    - B级威胁。有组织的分布式协同攻击，指多点、多技术协同攻击。这种攻击危害大，难以对付，经常攻击一些专用网络。
    - A级威胁。通常是指战争威胁，其攻击范围比B级更大，使用的攻击技术更全面，危害更大。

黑客攻击的手段

- 中断（攻击系统的可用性）；
- 窃听（攻击系统的机密性）；
- 篡改（攻击系统的完整性）；
- 伪造（攻击系统的真实性）；

电子商务安全保障的特殊性

- 除了具有一般信息安全的含义外，还具有金融业安全和商业信息安全的特征
- 系统的复杂性以及风险、威胁来源多样性带来安全保障的复杂性
- 信息资产的价值和敏感性高
- 涉及对象众多带来的管理难道非常大
- 是一个不断变化的安全过程

电子商务系统的核心保障目标

- 系统的可用性、可靠性与可控性
- 交易的安全性
  - 机密性
  - 完整性
  - 不可抵赖性
  - 可用性
  - 可审计性
- 参与各方私有信息的机密性
- 信息的真实性（公共电子商务平台系统）

电子商务安全术语

术语	定义
保密性（security）	保护机密信息不被非法存取以及信息在传输过程中不被非法窃取。
完整性（integrity）	防止信息在传输过程中丢失和重复以及非法用户对信息的恶意篡改。
认证性（authenticity）	确保交易信息的真实性和交易双方身份的合法性
可控性（access control）	保证系统、数据和服务能由合法人员访问
不可否认性（non-repudiation）	有效防止通信或交易双方对已进行的业务的否认

正确的安全理念

- 电子商务安全是系统性问题
  - 要综合考虑人、技术、管理、法规、制度等多项要素
- 电子商务安全安全是整体性问题
  - 指望几项离散的安全产品或技术手段解决所有安全问题是不现实的
- 安全保障是动态发展的过程
  - 安全保障建设不会是一劳永逸的
- 安全是相对性的
  - 安全保障建设投资是可度量的

电子商务的系统安全技术

- 病毒防范机制
- 网络层安全机制
  - 防火墙
  - 入侵检测
- 应用层安全机制
  - 数据加密
  - 认证技术
    - 报文认证
      - 数字签名
      - 数据完整性保护
    - 身份认证
  - 访问控制和路由控制
  - 安全审计

病毒防范机制

- 计算机病毒（Computer Virus）是编制或在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。
- 病毒的特征
  - ① 欺骗性。
  - ② 传染性。
  - ③ 潜伏性。
  - ④ 表现性。
  - ⑤ 可触发性。

病毒的分类

- 病毒的分类
  - 按寄生方式分为引导型病毒、文件型病毒和复合型病毒
  - 按破坏性分为良性病毒和恶性病毒
- 恶意代码
  - 蠕虫
  - 特洛伊木马
  - 逻辑炸弹

病毒防范

- 预防技术
- 检测病毒技术
- 杀毒技术

网络层防范机制

- 防火墙 ： 防火墙就是放在两个网络之间的各种系统组件的集合。例如，路由器、主计算机和适当软件的多种组合。
- 入侵检测系统：它从系统的控制点收集信息，并分析信息，检查系统中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全屏障，在不影响网络性能的情况下对网络进行检测，从而提供对内部攻击、外部攻击和误操作的实时保护。

防火墙技术

- ①包过滤型。它是在网络层中对数据包实施有选择的通过。依据系统内事先设定的过滤逻辑，检查数据流中每个数据包后，根据数据包的源地址、目的地址、所用的TCP端口与TCP链路状态等因素来确定是否允许数据包通过。
- ②代理服务型。它是由一个应用网关作为代理服务器，接受外来的应用连接请求，进行安全检查后，再与被保护的网络应用服务器连接，使得外部用户在受控制的前提下使用内部网络的服务。同样，内部网络到外部的连接也可以受到监控。
- 与包过滤型防火墙不同的是，内部网与外部网之间不存在直接的连接，同时提供日志及审计服务。应用网关的代理服务实体将对所有通过它的连接做出日志记录，以便对安全漏洞检查和收集相关的信息。

数据加密技术

- 传统加密技术
  - 替换加密
  - 转换加密
- 现代加密技术
  - 单密钥
  - 双密钥

替换加密

单字母加密方法

Caesar（恺撒）密码表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	D	E	F	G	H	I	J	K	L	M	N	O	P
明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

密钥为3

请同学计算，此时如果明文为beijing，密文呢？

- 单表置换密码
  - 置换表中的密文字符的顺序是：将密钥Key的字母先对应明文，再将26个字母按顺序列出（隐去已出现的字母）。
- 假设密钥Key是BEIJINGTSINGHUA，由此密码构造的字符置换表如下：

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	B	E	I	J	N	G	T	S	H	U	A	C	D
明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	F	K	L	M	O	P	Q	R	V	W	X	Y	Z

请同学计算，此时如果明文为beijing，密文呢？

- 多字母加密方法
  - 密钥是一组信息（一串字符）。同一个明文经过不同的密钥加密后，其密文也会不同。

Vigenere密码

M	i	n	f	o	r	m	a	t	i	o	n
Key	S	T	A	R	S	T	A	R	S	T	A
C	A	G	F	F	J	F	A	K	A	H	N

- 假设明文m=m1m2m3.....mn，密钥Key=K1K2K3.....Kn，对应密文C=C1C2C3.....Cn，
- 则：Ci =(mi + Ki) mod 26，i = 1，2，.....n，
- 其中，26个字母A——Z的序号对应是0——25，
- 如果m=information，Key=STAR，则C=AGFFJFAKAHN

- Vigenere密码的密钥长度若增加，破译的难度也将增加，若密钥的长度与明文的长度一样，而且是随机的，Vigenere密码可做到一次一加密。

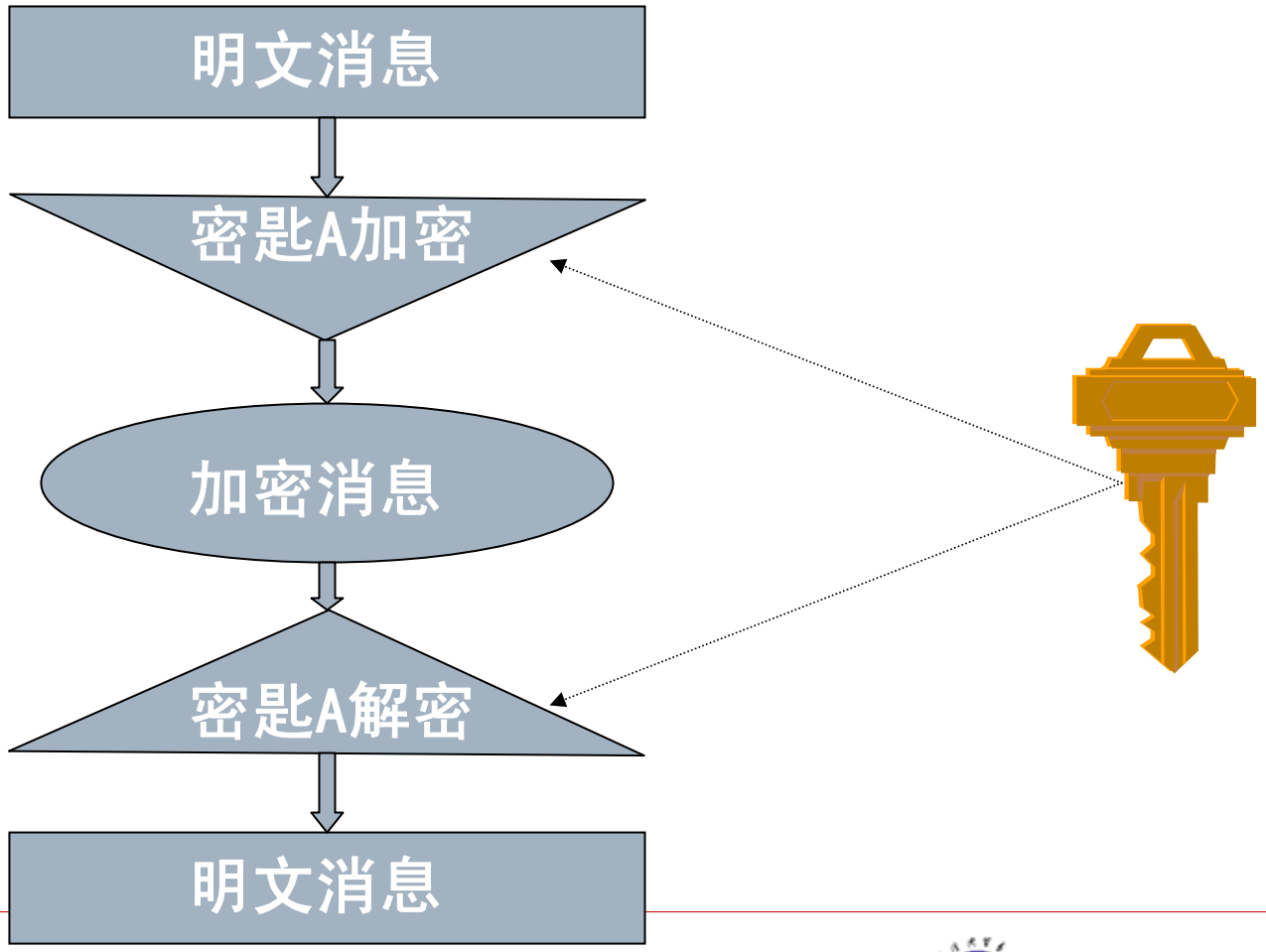
转换加密

- 在替换加密法中，原文的顺序没被改变，而是通过各种字母映射关系把原文隐藏了起来。转换加密法是将原字母的顺序打乱，将其重新排列。如：
  - it can allow students to get close up views
  - 将其按顺序分为5个字符的字符串：
  - itcan
  - allow
  - stude
  - ntsto
  - getcl
  - oseup
  - views
- 再将其按先列后行的顺序排列，就形成了密文：
  - 即密文C为“IASNGOVTLTTESICLUSTEEAODTCUWNWEOLPS”
- 如果将每一组的字母倒排，也形成一种密文：
  - C=NACTIWOLLAEDUTSOTSTNLCTEGPUESOSWEIV

数据加密技术

- 现代加密体制可以分为两种：单钥（对称）加密体制和双钥（非对称）加密体制。
  - 在单钥加密体制中，加密密钥和解密密钥是相同的。
  - 在双钥加密体制中，加密密钥和解密密钥不同，并且很难从一个推导出另一个，因此加密密钥（公钥）可以公开，解密密钥（私钥）由用户自己保存。这种加密算法可以满足网络系统开放性的要求，即当加密算法被公开时，不能通过加密密钥计算出解密密钥。

对称密匙加密



单密钥的特点

- 在首次通信前，双方必须通过除网络以外的另外途径传递统一的密钥。
- 当通信对象增多时，需要相应数量的密钥。
- 对称加密是建立在共同保守秘密的基础之上的，在管理和分发密钥过程中，任何一方的泄密都会造成密钥的失效，存在着潜在的危险和复杂的管理难度。

现代加密算法

- 单钥加密技术
  - DES
  - 单钥加密技术在电子商务交易过程中存在几个问题：

    ① 对称密钥的管理和分发；

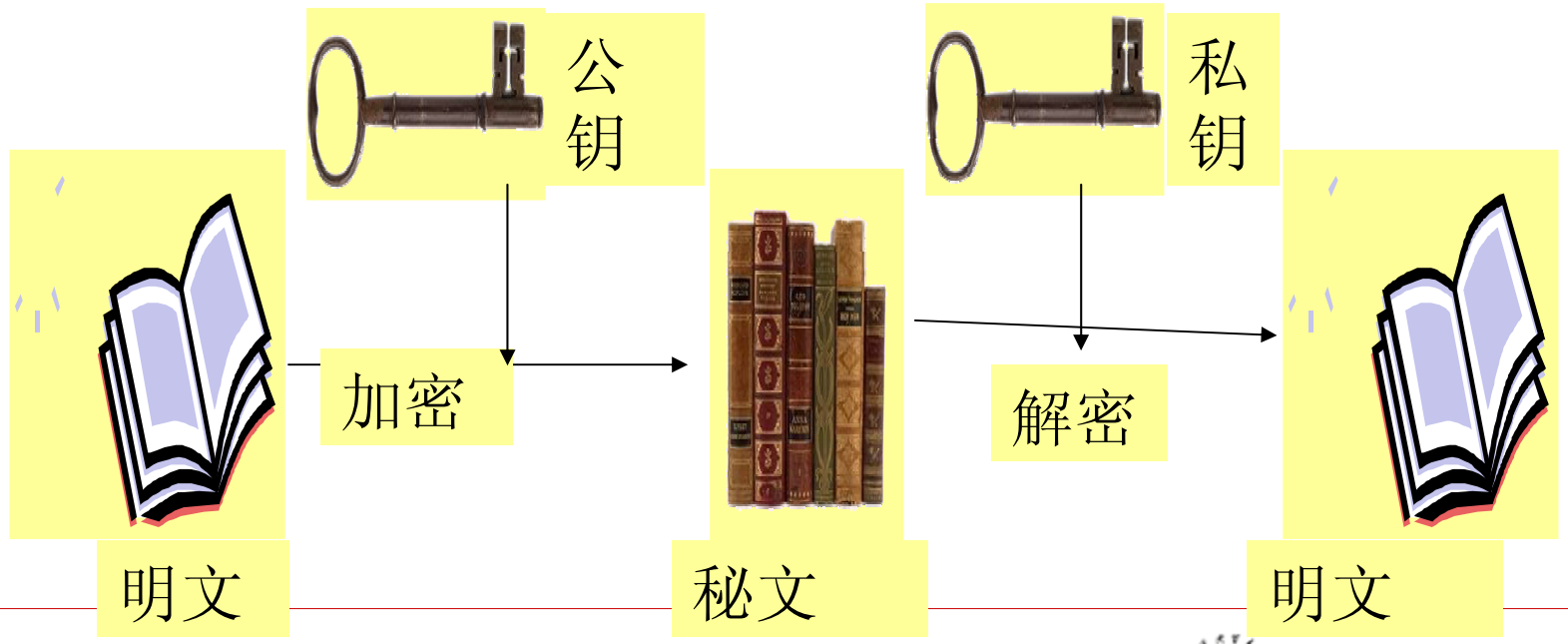
    ②电子商务中要求提供一条安全的渠道使交易双方在首次通讯时协商一个共同的密钥几乎是不现实而且难于实施的；

    ③ 密钥的数目难于管理；

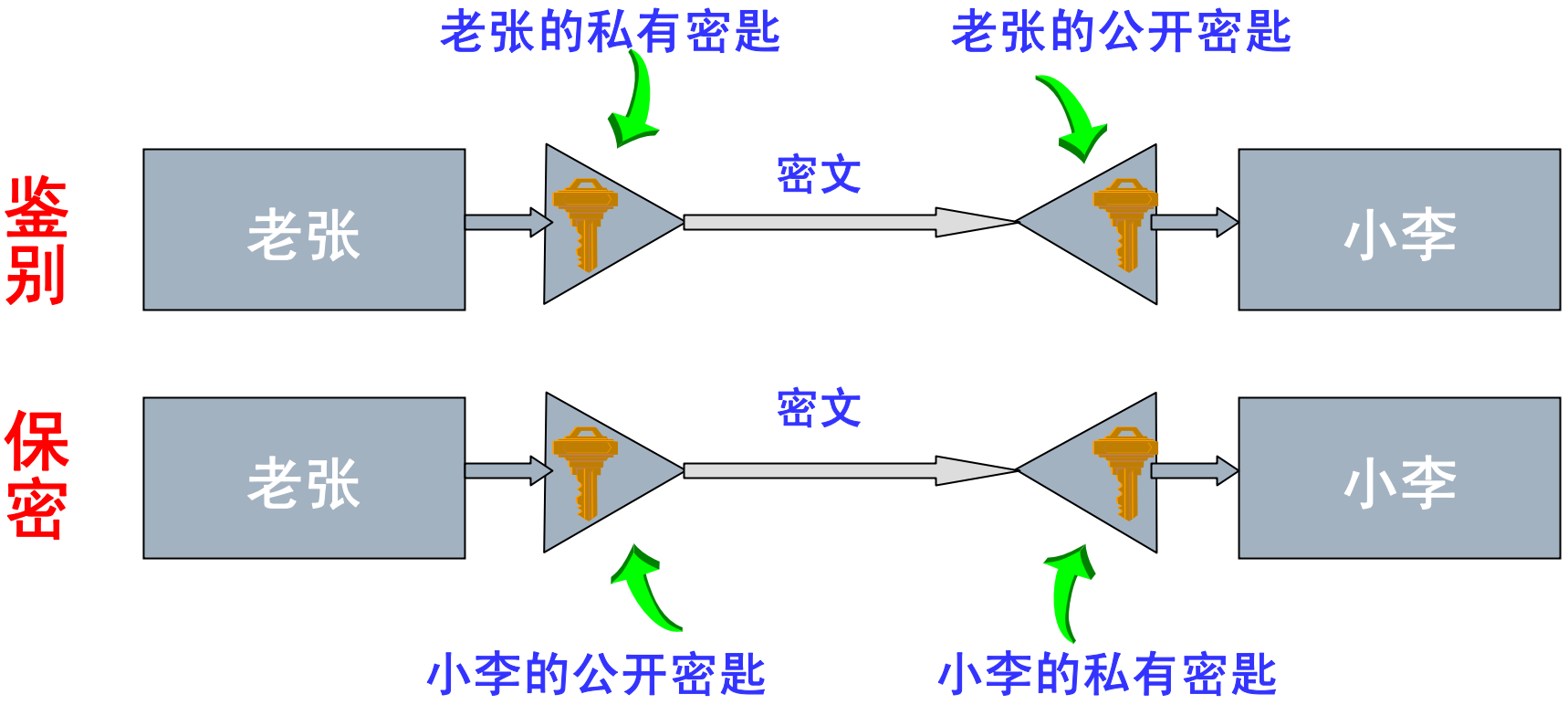
    ④ 对称加密算法一般不能提供信息完整性的鉴别，它无法验证发送者和接受者的身份。

双钥加密技术

- RSA
- 数学基础：大素数难分解



公开密匙/私有密匙加密



用RSA鉴别，只有老张能发出该信息

用RSA保密，只有小李能解开该信息

对称与非对称加密体制对比

特　　性	对　　称	非 对 称
密钥的数目	单一密钥	密钥是成对的
密钥种类	密钥是秘密的	一个私有、一个公开
密钥管理	简单不好管理	需要数字证书及可靠第三者
相对速度	非常快	慢
用途	用来做大量资料的加密	用来做加密小文件或对信息签字等不太严格保密的应用

实际应用(对称加密和非对称加密的使用)

- 发送方用对称密钥来加密数据，然后将此对称密钥用接收方的公开密钥加密，称为“数字信封”，将之和数据一起发送给接收方。
- 接收方先用相应的私有密钥打开数字信封，得到对称密钥，然后使用对称密钥解开数据。
- 这种技术的安全性能相当高，因为只有接收方才拥有自己的公开密钥，所以即使其他人得到了经过加密的对称密钥，也因为无法进行解密而保证了对称密钥的安全性，从而也保证了传输文件的安全性。

认证技术

- 报文认证
  - 报文认证用来保证通信双方的不可抵赖性和信息的完整性；
- 身份认证
  - 身份认证用来鉴别用户的身份。

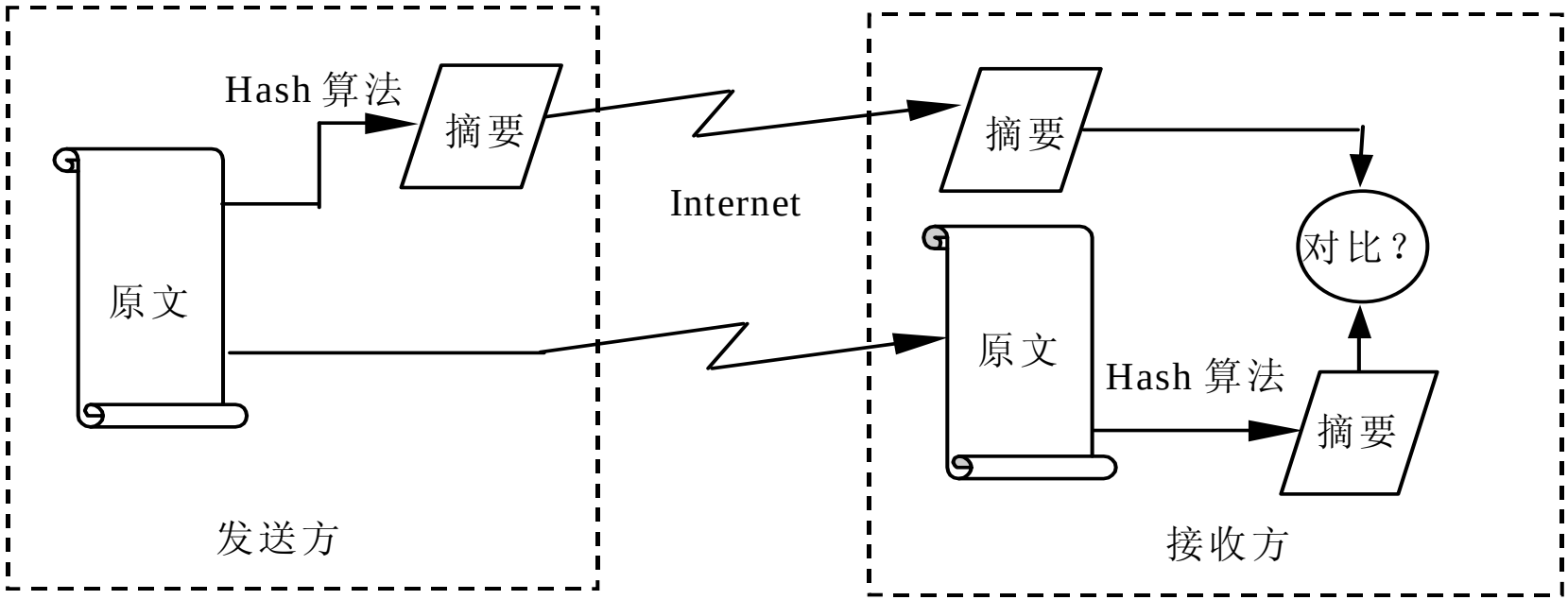
认证方法和手段

- 报文摘要
- 数字签名
- 数字时间戳
- 数字证书。

数据完整性机制:报文摘要

- 电子商务信息的完整性主要依靠报文摘要算法（Message Digest Algorithms），即采用单向散列（Hash）算法将需要加密的明文进行摘要，而产生的具有固定长度的单向散列值（或称报文摘要，Message Digest）。
  - 其中，散列函数（Hash Functions）是将一个不同长度的报文转换成一个数字串（即报文摘要）的公式，该函数不需要密钥，公式决定了报文摘要的长度。
  - 原理：这种方法主要是基于散列算法对于不同的数据产生相同散列值（或称报文摘要，Message Digest）的概率非常小。一旦数据信息遭到任何形式的篡改，必然产生不同的散列值，立刻检验出信息的完整性受到破坏，这样就防止非法用户对数据的篡改。

报文摘要



报文摘要过程

数字签名机制

- 数字签名（Digital Signature）机制由两个过程组成：对信息进行签名的过程和对已签名的信息进行证实的过程。
  - 前者要使用签名者的私有信息（如私有密钥）；
  - 后者使用公开信息（如公开密钥）进行解密，以鉴定签名者的身份，即签名是否由签名者私有信息产生。

数字签名和报文摘要技术

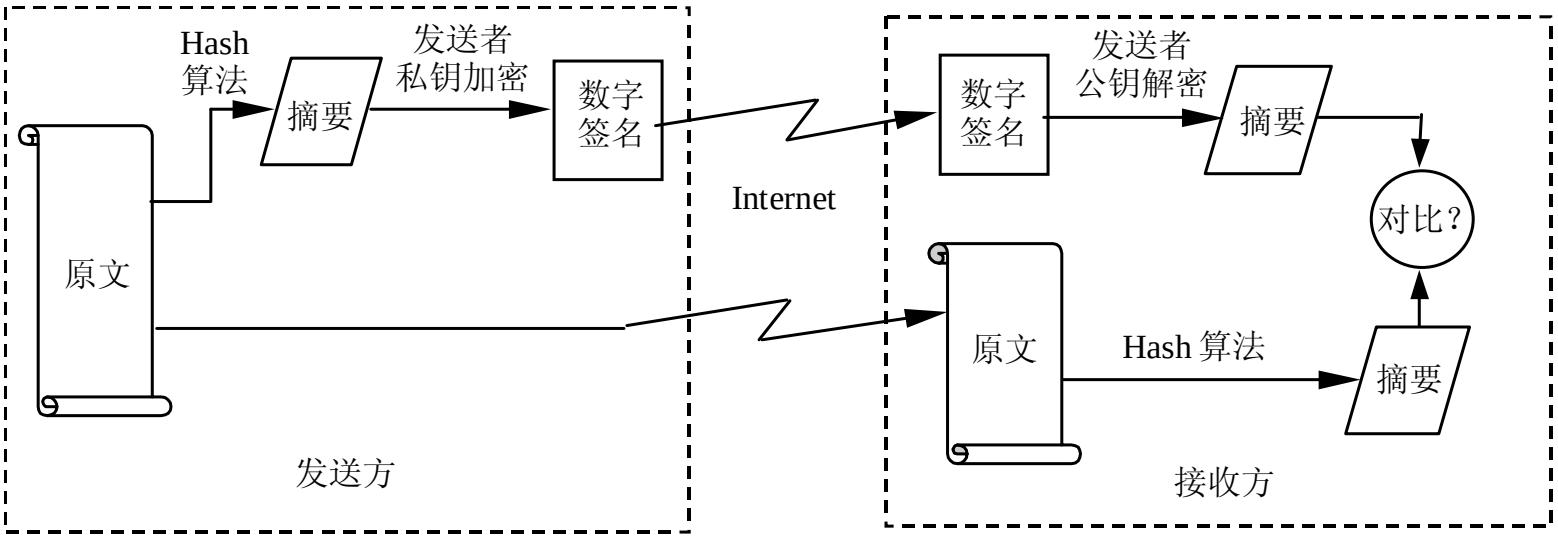
- 传统签名的意义
  - 签名使文件的接收者相信签名者是慎重地在文件上签字的；
  - 签名是签名者慎重地签在文件上的证明；
  - 签名是文件的一部分，其他的人无法将签名移到不同的文件中；
  - 文件签名后，不能改变；
  - 签名和文件是一个整体，签名者签名后难以否认，从而可以确认已签署的这一事实。

- 在计算机中签名的问题：
  - 首先计算机的数据容易复制，即使人的签名难以伪造(如手写签名的图形图像)，但把一个文件的有效签名移到另一文件中是轻而易举的事。
  - 签名后的文件修改也可以做到不留任何痕迹。

双重加密

- 数字签名和报文摘要相结合实现签名
  - 报文的发送方从报文文本中生成一个散列值(或报文摘要)，发送方用自己的私钥对这个散列值进行加密来形成发送方的数字签名。
  - 然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先从接收到的原始报文中计算出散列值(或报文摘要)，接着再用发送方的公钥来对报文附加的数字签名进行解密。
  - 如果两个散列值相同，证明报文具有完整性。同时，接收方通过该数字签名就能确认发送方的身份。
  - 因此，通过数字签名能够实现对原始报文完整性的鉴别和发送者对所发报文的不可抵赖性。

数字签名


Hash
算法
摘要
发送者
私钥加密
数字
签名
原文
发送方
Internet
数字
签名
发送者
公钥解密
摘要
对比？
原文
Hash 算法
摘要
接收方

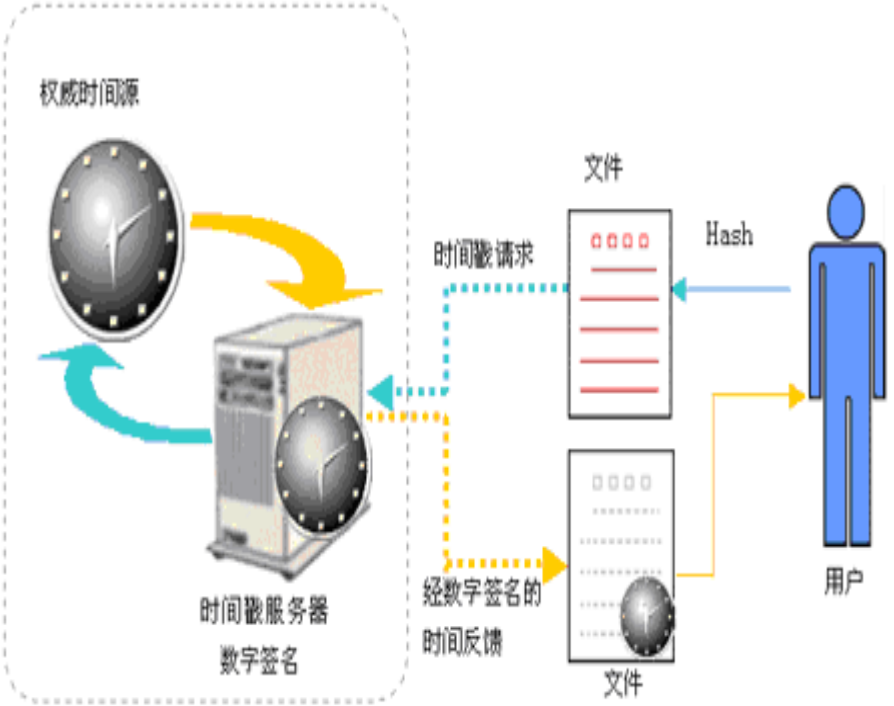
数字签名过程

数字时间戳

- 数字时间戳服务DTS(digital time-stamp service)是提供确认电子文件发表时间的安全保护。
- DTS必须由专门的服务机构来提供。
- 时间戳是一个经加密后形成的凭证文件，它由三部分组成：
  （1）需加时间戳的文件摘要；
  （2）DTS收到文件的日期和时间；
  （3）DTS的数字签名。

数字时间戳工作流程

（1）用户对文件数据进行Hash摘要处理；
（2）用户提出时间戳的请求，Hash值被传递给时间戳服务器；
（3）时间戳服务器对Hash值和一个日期/时间记录进行签名，生成时间戳；
（4）时间戳数据和文件信息绑定后返还，用户进行下一步网上交易操作。



数字证书

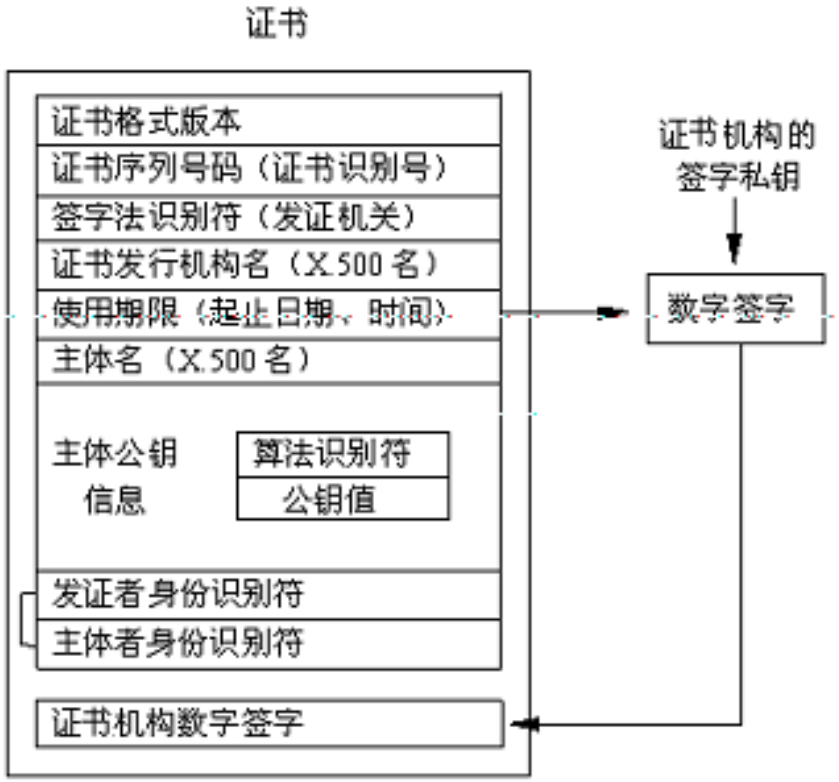
- 数字证书（digital certificate，digital ID）也称数字凭证，是用电子手段来标识一个用户的身份以及对网络资源访问权限的一系列数据。数字证书是由一个权威机构发行，它的作用与现实生活中的身份证类似。
- 分类
  - 个人凭证(personal digital ID)
  - 企业(服务器)凭证(server ID)
  - 软件开发者凭证(developer ID)

数字证书的机理

- 数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定另一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份机密信息时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。

数字证书的内部格式

- CCITT X.509国际标准
- 一个标准的X.509数字证书包含以下一些内容
  - 证书的版本信息；
  - 证书的序列号；
  - 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；
  - 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。



认证中心（CA）

- 认证中心主要负责电子商务安全交易的认证服务，主要负责产生、分配和管理用户的数字证书。
- 树状结构
  - 各级认证机构按照根认证中心（Root CA）
  - 品牌认证中心（Brand CA）
  - 持卡人、商户或收单银行的支付网关认证中心（Holder Card CA，Merchant CA 或 Payment Gateway CA）
  - 由上而下按层次结构建立的

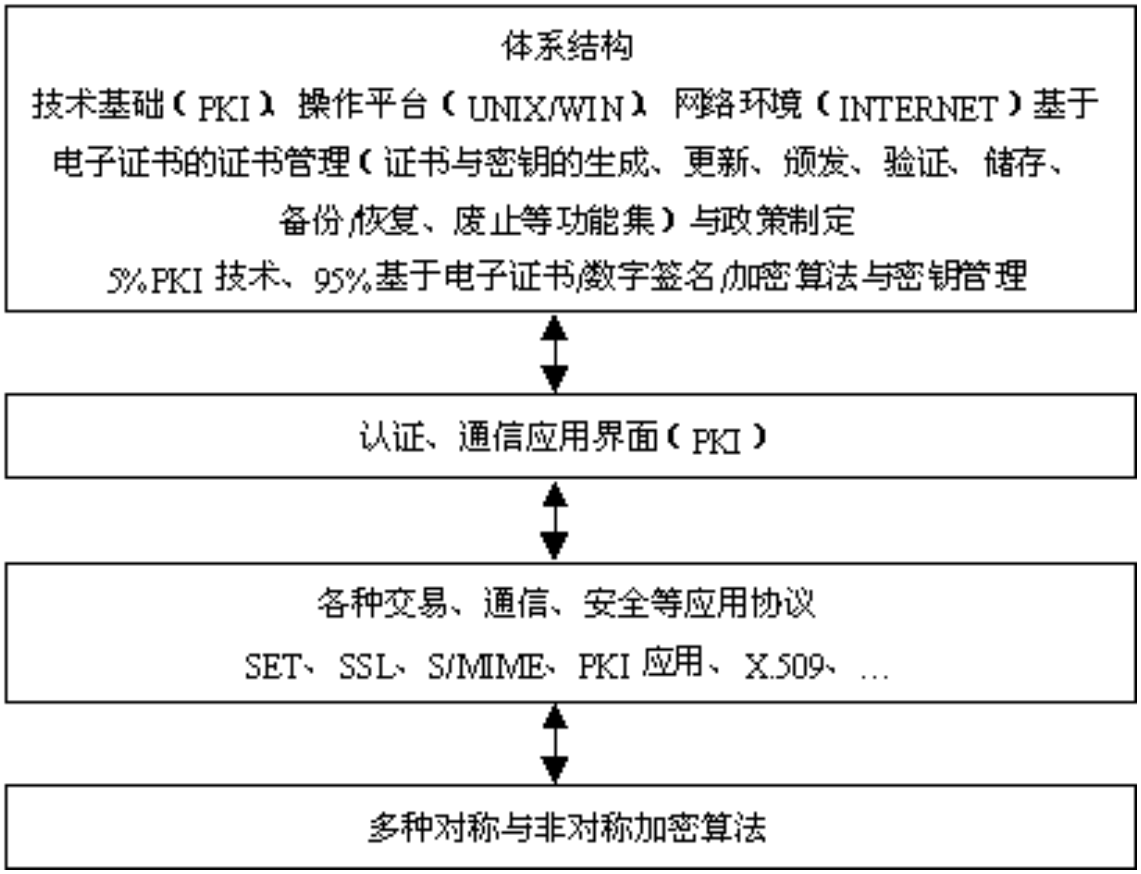
数字证书的发行与管理的主要过程

- （1）证书申请
- （2）主体认证
- （3）证书生成
- （4）证书更新
- （5）证书撤销
- （6）证书验证

PKI：综合利用上述技术的安全体系

- PKI（Public Key Infrastructure ）是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。用户可利用PKI平台提供的服务进行安全的电子交易，通信和互联网上的各种活动。
- PKI（公钥基础设施）技术采用证书管理公钥，通过第三方的可信任机构--CA认证中心把用户的公钥和用户的其他标识信息捆绑在一起，在互联网上验证用户的身份。目前，通用的办法是采用建立在PKI基础之上的数字证书，通过把要传输的数字信息进行加密和签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。PKI是基于公钥算法和技术，为网上通信提供安全服务的基础设施。是创建、颁发、管理、注销公钥证书所涉及到的所有软件、硬件的集合体。其核心元素是数字证书，核心执行者是CA认证机构。
- PKI的基础技术包括加密、数字签名、数据完整性机制、数字信封、双重数字签名等。

公钥基础结构 （PKI ）


体系结构
技术基础（PKI） 操作平台（UNIX/WIN） 网络环境（INTERNET）基于
电子证书的证书管理（证书与密钥的生成、更新、颁发、验证、储存、
备份/恢复、废止等功能集）与政策制定
5%PKI 技术、95%基于电子证书/数字签名/加密算法与密钥管理
认证、通信应用界面（PKI）
各种交易、通信、安全等应用协议
SET、SSL、S/MIME、PKI 应用、X.509、…
多种对称与非对称加密算法

PKI的性能

- 支持多政策
- 透明性和易用性
- 互操作性
- 支持多平台
- 支持多应用

访问控制和路由控制

- 访问控制机制是根据实体身份及有关信息，来决定该实体的访问权限。它按照事先确定的规则决定主体对客体访问是否合法。
- 在大型的网络中，数据从源节点可能有多条线路可以到达目的节点，其中，有些线路可能是安全的，而另一些线路是不安全的。
- 路由控制机制可使信息发送者选择特殊的路由申请，以保证数据安全。为了使用安全的子网、中继站和链路，即可预先安排网络中的路由，也可根据安全策略动态选择

防业务流分析机制

这种机制主要对抗非法者对线路上的数据监听，并对其进行流量和流向分析。采用的解决方法一般是由保密装置在无信息传输时，连续地发出伪随机信息序列，使非法者不知哪些是有用的信息，哪些是无用的信息。

安全审计跟踪

- 安全审计就是对系统的记录与行为进行独立的评估考察，目的是测试系统的控制是否得当，是否能保证与既定策略协调一致。
- 安全审计还能提供一种事后的安全漏洞检测，对潜在的安全攻击起到威慑作用。

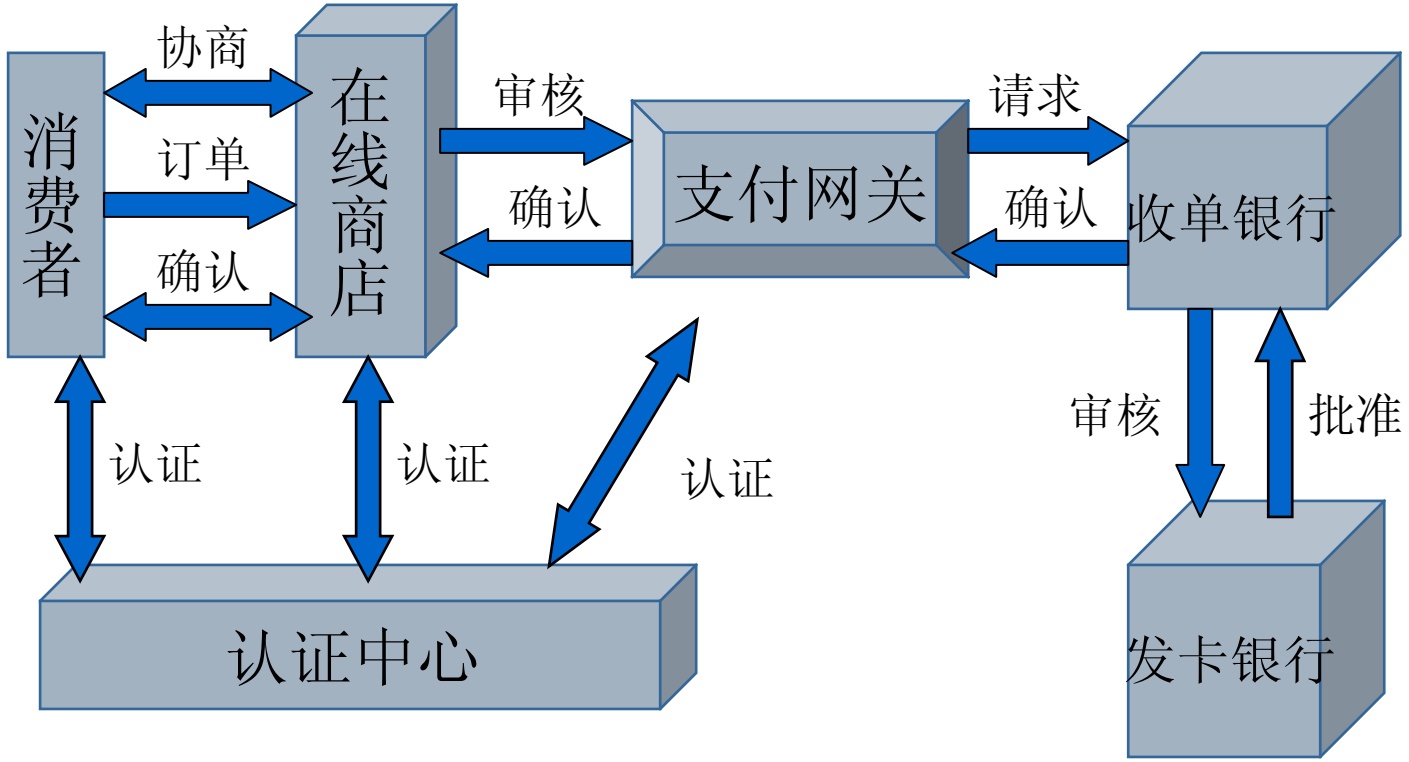
电子商务安全交易协议

- 安全电子交易协议SET
- 安全套接层协议SSL

安全电子交易协议(SET)

- 安全电子交易(Secure Electronic Transaction)协议是由VISA、MasterCard两大信用卡公司以及IBM等公司共同推出的用于开放网络进行安全资金支付的技术标准
- 初衷是将传统的信用卡交易模式移植到互联网上，同时又保证这种新的交易方式有足够的安全性
- SET协议要解决持卡人、商家和银行三角关系的单向或双向的安全数据传输和对方身份认证等一系列安全问题。

SET安全技术



SET中的用户角色

- 消费者：购买者通过计算机与商家交流，通过由发卡机构颁发的付款卡进行结算。在与商家的会话中，SET可保证消费者的个人账号信息不被泄露。
- 发卡机构：一个金融机构，为每一个建立了账户的顾客颁发付款卡。
- 商家：提供商品或服务，使用SET可以保证消费者信息的安全。接受卡支付的商家必须和银行有关系。
- 银行：在线交易的商家在银行开立账号，并且处理支付卡的认证和支付。
- 支付网关：由银行操作的，将Internet上的传输数据转换为金融机构内部数据的设备，或由指派的第三方处理商家支付信息和顾客的支付指令。

SET安全技术的特点

（1）信息的机密性

发送方将消息用DES加密，并将DES对称密钥用接受方的公钥加密，称为消息的“数字信封”，将数字信封与DES加密后的消息一起发给接受方。接受者收到消息后，先用其密钥打开数字信封，得到发送方的DES对称密钥，再用此对称密钥去解开数据，确保了信息的机密性。

（2）信息的私密性

SET的一个重要特点是持卡人的信用卡号码只提供给银行，而商家无法知道信用卡号码。在交易中持卡人发往银行的支付指令是通过商家转发的，为了避免在交易的过程中商家窃取持卡人的信用卡信息，以及避免银行跟踪持卡人的行为，侵犯消费者隐私，但同时又不能影响商家和银行对持卡人所发信息的合理的验证，只有当商家同意持卡人的购买请求后，才会让银行给商家负费，SET协议采用双重签名来解决这一问题。

- 假设持卡人C从商家M购买商品，他不希望商家看到他的信用卡信息，也不希望银行B看到他有关商品的信息，于是他采用双重签名，流程说明如下：
- 首先C产生发往M的订购信息OI和发往B的支付指令PI，并分别产生OI，PI的摘要H(OI)，H(PI)，用摘要可以检查消息在中途是否被篡改。连接H(OI)和H(PI)得到OP，再生成OP的摘要H(OP)，用C的RSA私钥签名H(OP)，得sign[H(OP)]，称为双重签名。C将消息{OI，H(PI)，sign[H(OP)]}发给M，将{PI，H(OI)，sign[H(OP)]}发给B。

- 在验证双重签名时，接受者分别创建消息摘要，M生成H(OI)，B生成H(PI)，再分别将H(OI)/H(PI)与另一接受到的摘要H(PI)/H(OI)连接，生成OP及其摘要H(OP)’，接受者M/B用C的RSA公钥解开sign[H(OP)]，得到H(OP)，比较H(OP)’与H(OP)是否相同，如果相同，则表示数据完整且未被篡改，如果不同，则丢弃数据。

（3）数据的完整性

从持卡人发往商家的支付信息包括订购信息、个人数据及支付指令。SET引入RSA数字签名及Hash散列算法确保这些消息的内容在传输过程中不被非法更改。

（4）持卡人/商家身份的鉴别

SET可以让商家鉴别持卡人是否是有效信用卡账户的合法用户，并且让持卡人可以鉴别商家真实性，而且可以验证商家能否接受信用卡支付。SET采用X.509数字证书达到这一目的。

（5）发送方的不可抵赖

SET引入RSA数字签名，数据发送方采用自己的私钥加密数据，接受方用发送方的公钥解密，保证了发送方不能抵赖发送过数据，完全模拟了现在生活中的签名。

SET安全支付的流程

（1）持卡人向商家发初始请求，商家产生初始应答。

持卡人浏览商家的商品，选好商品后要求在线支付，激发支付软件，向商家发送初始请求。初始请求指定了交易环境，包括持卡人所使用的语言，交易ID，使用的是何种交易卡等。商家接受初始请求，产生初始应答，对初始应答生成消息摘要，对此消息摘要进行数字签名，将商家证书，网关证书，初始应答，消息摘要的数字签名等，发送给持卡人。由于初始应答未被加密，所以它不应包含机密信息。

（2）持卡人接受并检查商家的初始应答，如无误，发出购物请求。

持卡人接受初始应答，检查商家证书和网关证书。接着用商家公钥解开消息摘要的数字签名，用Hash算法产生初始应答的摘要，将两者比较，如果相同则表示数据在途中未被篡改，否则丢弃。

持卡人发出购物请求，它包含了真正的交易行为。购物请求是协议中最复杂的信息，它包括两个部分：发往商家的定单指令OI和通过商家转发往网关的支付指令PI，通过双重签名将PI和OI结合起来，生成 sign[H（OP）]。持卡人生成对称密钥，对支付指令PI加密，再用网关的公钥对此对称密钥和持卡人账号加密，形成数字信封。最后将持卡人证书，OI，PI密文，数字信封，sign[H（OP）]，PI和OI各自的消息摘要等发给商家，其中有消息是通过商家转发给支付网关的。

（3）商家接受并检查持卡人的购物请求，如无误，发出支付请求。

商家接受持卡人的购物请求，认证持卡人的证书。接着验证双重签名，看数据在传输过程中是否被篡改。如数据完整，则处理定单信息，产生支付请求。

将支付请求用Hash算法生成摘要，并签名，网关收到后用商家公钥解密，并确认支付请求是此商家所发在且在途中未被篡改。生成对称密钥对支付请求加密，并用网关公钥加密形成数字信封。最后将商家证书，支付请求密文，商家数字签名，数字信封和持卡人通过商家转发的：sign[H（OP）]，OI摘要，PI密文，持卡人数字信封，持卡人证书等发往支付网关。

（4）支付网关接受并检查支付请求，如无误，发扣款请求。

支付网关分别检查确认商家发来的数据和持卡人发来的数据。网关首先认证商家证书，然后用私钥打开商家数字信封，获取商家对称密钥， 解开支付请求密文。用Hash算法作用于支付请求，形成摘要，与商家发来的支付请求摘要（解开数字签名所得）相比较，如果相同则表示数据完整，否则丢弃数据。

网关检查持卡人证书，然后用私钥打开持卡人数字信封，得到他的账号和对称密钥。用此对称密钥解开PI密文，得到PI，接着验证双重签名，生成PI的摘要，与OI摘要相连接，再次生成摘要，其结果与H（OP）(解双重签名所得)相比较，如果相同则数据完整，如果不同则丢弃。网关将信息发送往银行。

（5）银行向网关发送扣款应答，网关向商家发送支付应答。

在支付网关和银行之间是通过金融专用网相连，其间的业务，SET并不作规定。

网关在接受银行的扣款应答后，生成支付应答，同样产生摘要，对其进行数字签名，生成对称密钥，对支付应答加密，并且将对称密钥装入数字信封。将网关证书，数字签名，数字信封，支付应答密文一起发往商家。

（6）商家接受并检查网关的支付应答，如无误，向持卡人发送购物应答。

商家认证网关的证书，用私钥打开数字信封，得到网关对称密钥，用此密钥解开支付应答，产生摘要。用网关公钥解开其数字签名，得到支付原始支付应答摘要，并与新产生的摘要比较，如果相同，则数据完整，如果不同则丢弃。

商家产生购物应答，对购物应答生成摘要，并签名，将商家证书，购物应答，数字签名一起发往持卡人。如果交易成功，则发货。

持卡人接受购物应答，验证商家证书。对购去应答产生摘要，用商家公钥解开数字签名，得到原始摘要，将之与新产生的摘要比较，相同则表示数据完整，不同则丢弃。至此，交易流程结束。

安全套接层协议

- 在浏览器和服务器产品之间提供安全通信。

SSL安全技术的特点

SSL将对称加密技术和非对称加密技术相结合。在建立连接过程中采用非对称加密技术，在会话过程中使用对称加密技术。可以在任何两个通信应用中提供机密性、完整性、身份鉴别服务，保证了客户和服务器间事务的安全性。

（1）信息的机密性。SSL客户机和服务器之间通过密码算法和密钥的协商，建立起一个安全通道，以后在安全通道中传输的所有信息都经过了加密处理，网络中的非法窃听者所获取的信息都将是无意义的密文信息。

（2）数据的完整性。SSL利用加密技术和散列函数，通过对传输信息特征值的提取来保证信息的完整性，确保要传输的信息全部到达目的地，可以避免服务器和客户机之间的信息内容受到破坏。

（3）消费者/商家身份鉴别。即客户机和服务器相互识别的过程。它们的识别号用公开密钥码，并在SSL握手中交换各自的识别号。这样就可防止其它用户冒名顶替。

SSL安全支付的流程

- 六个阶段：

  （1）建立连接阶段：消费者通过网络向商家打招呼，商家回应；

  （2）交换密码阶段：消费者与商家之间交换双方认可的密码；

  （3）会谈密码阶段：消费者与商家之间产生彼此交谈的会谈密码；

  （4）检验阶段：检验商家取得的密码；

  （5）消费者认证阶段：验证消费者的可信度；

  （6）结束阶段：消费者与商家之间相互交换结束信息。

SSL和SET的区别

- SSL是基于传输层的通用安全协议，它只占电子商务体系中的一部分，是对数据传输的那部分技术规范。
- SET协议位于应用层，对其他各层也有涉及。SET中规范了整个商务的活动流程。持卡人、商家、支付网关、结算中心、认证中心之间的信息流的加密、认证，SET协议都制定了严密的标准。

电子商务安全管理

- 1. 电子商务安全管理的主要内容
  - 安全管理是实现电子商务系统信息安全的落实手段，也是一项技术性强、涉及面广的管理工作。其主要内容包括：人事管理、设备管理、场地管理、存储设施管理、软件管理、网络管理和密码、密钥管理。
- 2. 安全管理的基本原则
- 3. 安全管理的应急处理

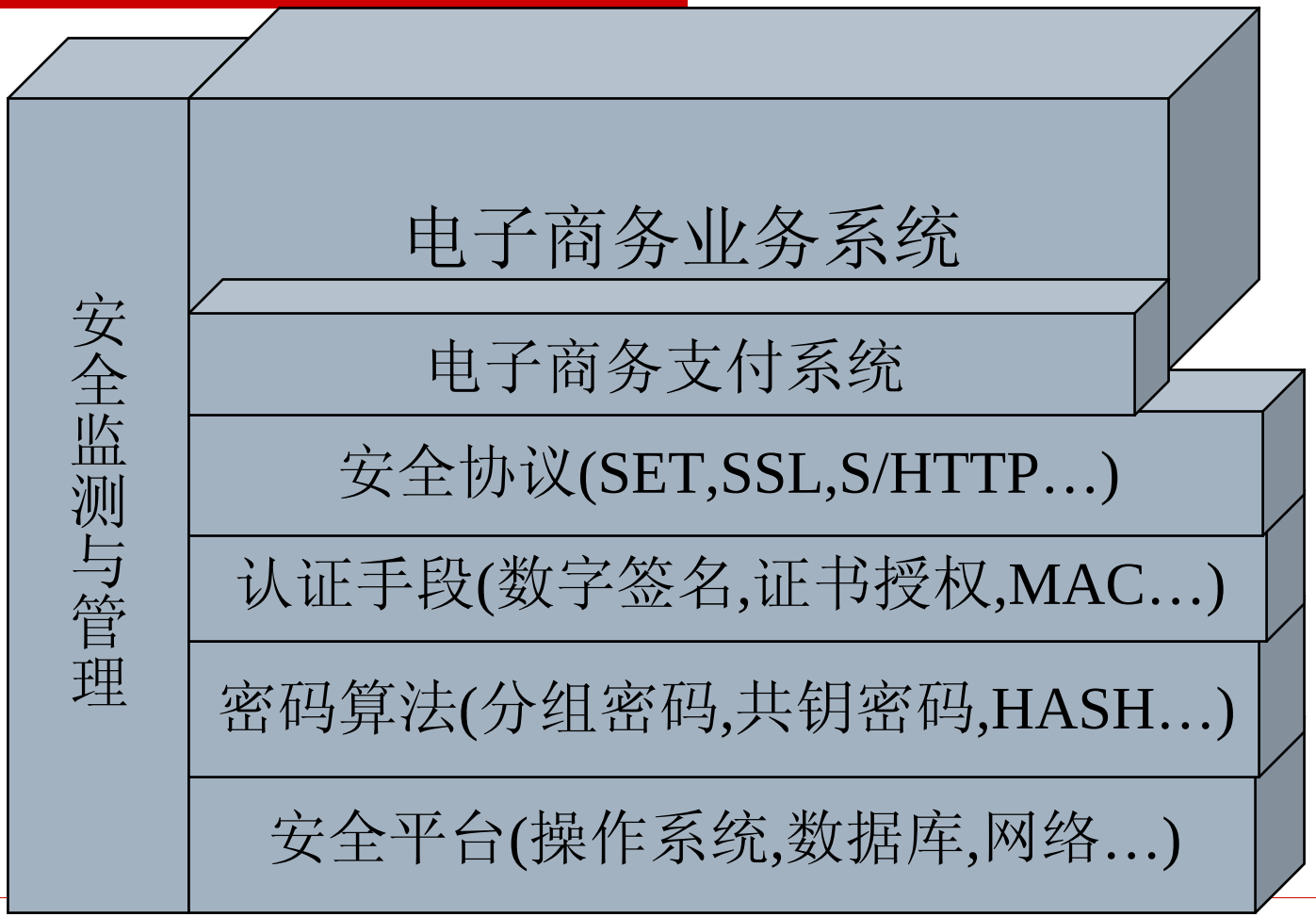
安全管理的基本原则

- （1）规范原则
- （2）预防原则
- （3）选用成熟技术原则
- （4）系统化原则
- （5）分权制约原则
- （6）应急原则
- （7）灾难恢复原则

安全管理的应急处理

- （1）分析判断
- （2）入侵或攻击的终止
- （3）记录和备份
- （4）恢复
- （5）定位
- （6）汇报

小结


电子商务业务系统
电子商务支付系统
安全协议(SET,SSL,S/HTTP…)
认证手段(数字签名,证书授权,MAC…)
密码算法(分组密码,共钥密码,HASH…)
安全平台(操作系统,数据库,网络…)
安全监测与管理

7.4 电子商务安全解决方案

- B2B电子商务系统功能设计
  - 产品销售系统
  - 采购供应系统

思考：B2B电子商务的安全需求

- 网络层的安全需求
- 应用层的安全需求
- 后台管理的安全需求

B2B电子商务的整体安全解决方案

- 网络层安全解决方案
  - 安全网络结构设计
  - 防火墙技术与产品
  - 入侵检测技术与产品
  - 防病毒技术与产品

应用层安全解决方案

- 双向身份认证
- 对象访问控制
- 数据传输加密
- 审计日志服务
- 安全管理服务

- 安全的后台管理
  - 来自管理员的安全风险
- B2B电子商务内部CA解决方案
  - CA服务器
  - CA管理客户端
  - CA维护客户端