



第三讲 电子商务安全技术

北京大学计算机系电子商务实验室



4.1 电子商务系统安全问题概述

4.2 电子商务安全技术

4.3 电子商务安全交易标准

4.4 黑客攻击防范措施



4.1 电子商务系统安全问题概述


■ 4.1.1 网络安全的基本概念

- **密码安全**：通信安全的核心，正确使用强韧的密码系统
- **计算机安全**：一种确定的状态，使计算机数据和程序不被非授权人员、计算机或其它程序所访问、获取、修改。具体实施包括：
 - 限制被授权人员使用计算机系统的物理范围；
 - 利用特殊（或专用）软件；
 - 将安全功能构造于计算机操作规程中。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

3




■ 4.1.1 网络安全的基本概念

- **网络安全**：包括所有保护网络的措施：物理设施、软件及职员的安全，以防止非授权的访问或蓄意的干扰和破坏。因此有效的安全措施是技术与人事管理的一种均衡。
- **信息安全**：保护信息财富，使之免遭偶发或有意的非授权泄露、修改、破坏或处理能力的丧失。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

4




2002-3-23

■ 4.1.2 电子商务安全的重要性

- 电子商务安全是电子商务的生存保障
- 电子商务安全涉及国家经济安全

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

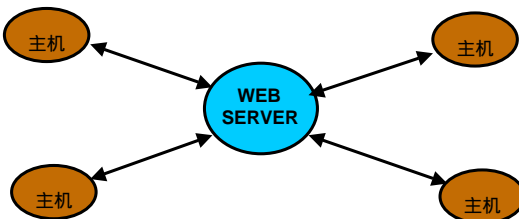
5



2002-3-23

DoS(Denial of Service)攻击

■ 2000年2月, eBay, Amazon, Yahoo, Etrade, buy.com, CNN, 其 Webserver在几小时之内由于无法处理众多请求而陷于瘫痪; 损失超过\$20亿美元。



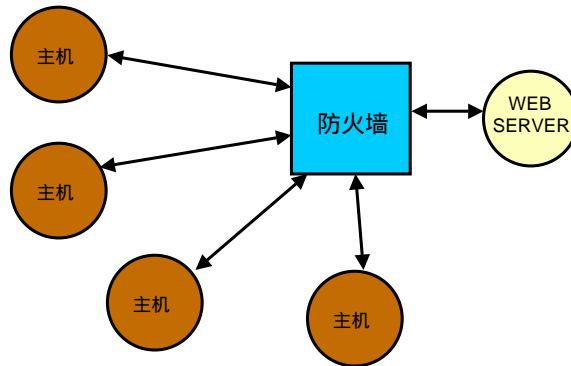
```
graph TD; H1((主机)) --> WS((WEB SERVER)); H2((主机)) --> WS; H3((主机)) --> WS; H4((主机)) --> WS;
```

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

6

分布的DoS

- 许多分布的用户发出服务请求，而均被示为合法而造成防火墙瘫痪



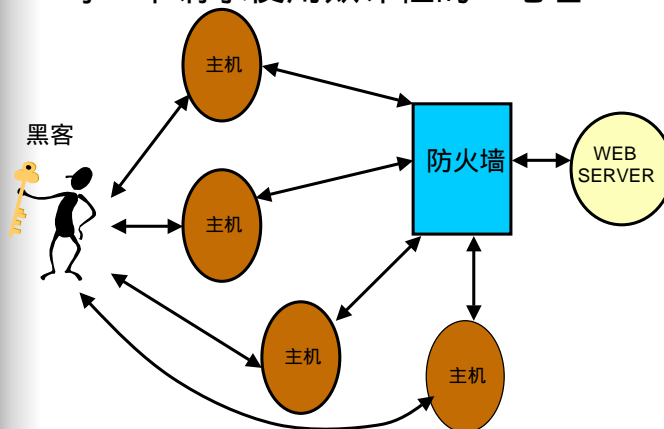
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

7

分布的DoS


- 请求来自由黑客安放的Daemon程序
- 每一个请求使用欺诈性的IP地址



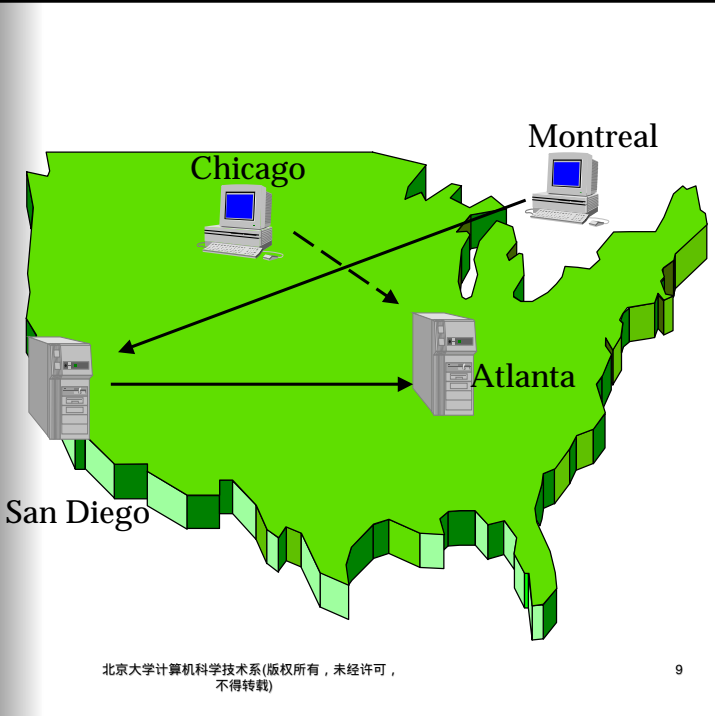
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

8



2002-3-23



Chicago

Montreal

Atlanta

San Diego

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

9



2002-3-23

■ 4.1.3 网络安全及对策

- 1. 网络安全体系结构



信息安全

网络安全

计算机安全

密码安全

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

10



● 2. 网络信息安全的基本要求

所谓网络信息安全，一般是指在信息的采集、存储、处理、传播和运用过程中，信息的保密性，完整性等特性都能得到良好保护的一种状态。

- **保密性** (Confidentiality, 即机密性, 如信用卡加密)
- **认证性** (Authentication, 即身份识别的真实性, 如购物者和商家的证明文件)
- **完整性** (Integrity, 如未经授权的篡改)
- **可访问性** (Accessibility, 如未经授权的存取)
- **防御性** (Defensibility, 如对信息资源的不当使用)
- **不可否认性** (Non-Repudiation, 如交易信息的可查性)

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

11



● 3. 面临的威胁

- **从纯技术的角度看**
 - 网络部件的不安全因素
 - 软件的不安全因素
 - 工作人员的不安全因素
 - 环境因素

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

12




2002-3-23

- 从商业运作的角度看
 - 卖方（销售者）面临的安全威胁
 - 系统中心安全性被破坏
 - 竞争者的威胁
 - 商业机密的安全
 - 假冒的威胁
 - 信用的威胁
 - 买方（消费者）面临的安全威胁
 - 虚假订单
 - 付款后不能收到商品
 - 机密性丧失
 - 拒绝服务（DoS）

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

13



2002-3-23

- 4. 对策
 - 技术对策

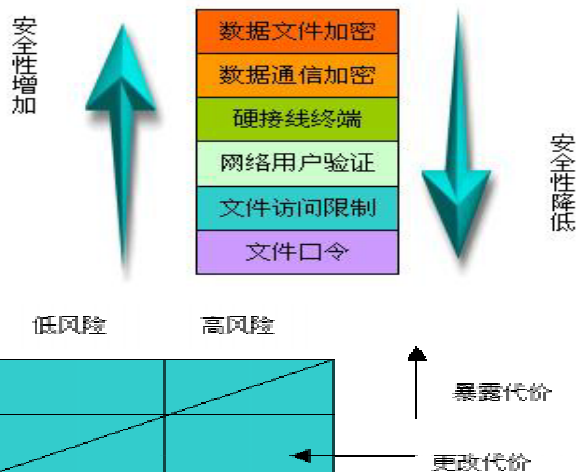
网络安全检测设备（SAFT suite）；访问设备（安全认证卡）；浏览器/服务器软件（支持SSL）；证书（VeriSign）；商业软件（支持电子支付）；防火墙等。
 - 管理对策

人员管理制度；保密制度；跟踪、审计、稽核制度；网络系统的日常维护制度；病毒防范措施；应急措施。

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

14

● 5. 网络通信安全的分层以及OSI安全体系结构



2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

15


■ OSI的安全体系结构

OSI的层	保密性	鉴别	数据完整性	不可抵赖	访问控制
应用	Y	Y	Y	Y	Y
表示	Y	Y	-	-	-
会话	-	-	-	-	-
传输	Y	Y	Y	-	Y
网络	Y	Y	Y	-	Y
链路	Y	-	-	-	-
物理	Y	-	-	-	-

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

16




- 6. 电子商务系统的安全体系结构
 - **支持服务层**：密码服务、通信、归档、用户接口和访问控制；
 - **传输层**：发送、接收、组织商业活动所需的封装数据条（如签名文本、证书、收据、已签名的陈述、数字化的商品等），此层包括付款模块、文档和证书服务模块；
 - **交换层**：提供封装数据的公平交换服务。
 - **商务层**：提供商业方案。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

17



4.2 电子商务安全技术

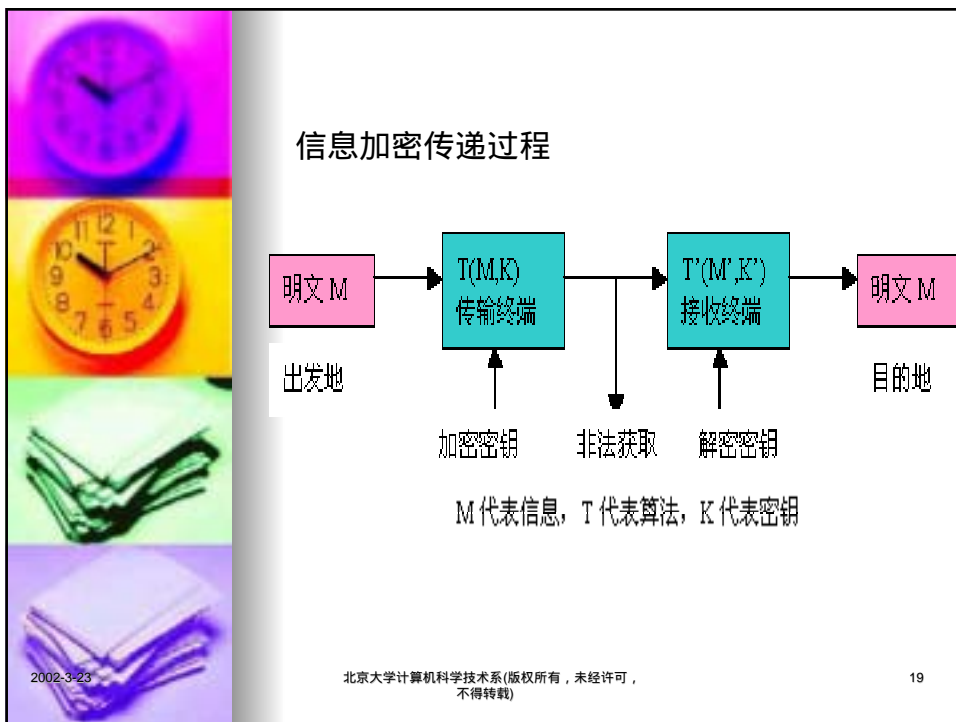
- 4.2.1 加密技术
 - 1. 基本概念

所谓信息加密技术，就是采用数学方法对原始信息（通常称为“明文”）进行再组织，使得加密后在网络上公开传输的内容对于非法接收者来说成为无意义的文字（加密后的信息通常称为“密文”）。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

18



古典加密解密方法

加密模型: $m \xrightarrow{k} c \xrightarrow{k} m$

单钥体制: $k = k$, 双钥体制: $k \neq k$


凯撒密码:

明文—ABCDEFGHIJKLMN...
 密钥—defghijklmnopqrs...
 密钥—keyabcdefghijklmnop...
 实例: CHINA fkl qd/yefkk

换位密码:

明文—COUNTRY SECURITY
 分组—COUNT RYSEC URITY
 密文—CRU OYR USI NET TCY

2002-3-23 北京大学计算机科学技术系(版权所有, 未经许可, 不得转载) 20



古典加密解密方法


棋盘密码:

4	6	1	8	7	5	2	0	9	3
6	a	b	c	d	e	f	g	h	i
3	k	l	m	n	o	p	q	r	s

明文--information security
密文—69386537303164.....

矩阵密码: $MA = C$ $M = CA^{-1}$

2002-3-23 北京大学计算机科学技术系(版权所有, 未经许可, 不得转载) 21



● 2.密码体制分类

- 私钥(单钥或对称)加密体制

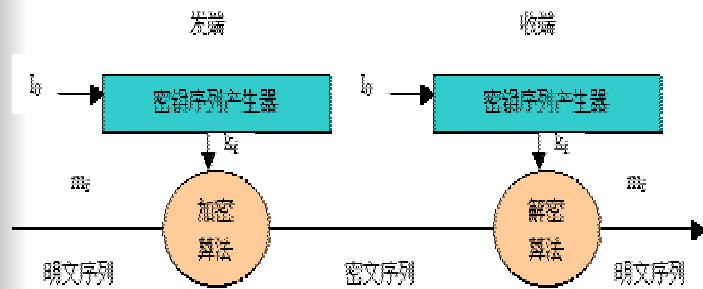
这种体制的加密密钥和解密密钥相同或者本质上相同(即从其中一个可以很容易地推出另一个)。

根据加密模式的不同, 又可分为两种:

- 序列密码
- 分组密码

2002-3-23 北京大学计算机科学技术系(版权所有, 未经许可, 不得转载) 22

▪ 序列密码加密和解密过程

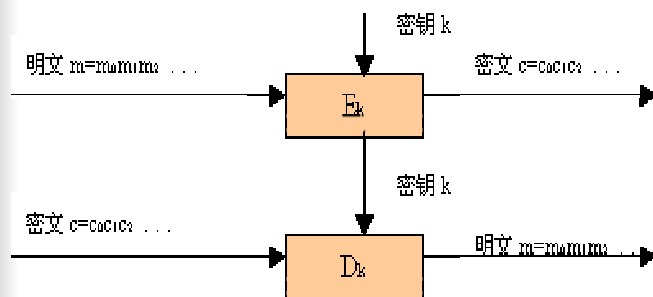


2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

23

▪ 分组密码的工作原理



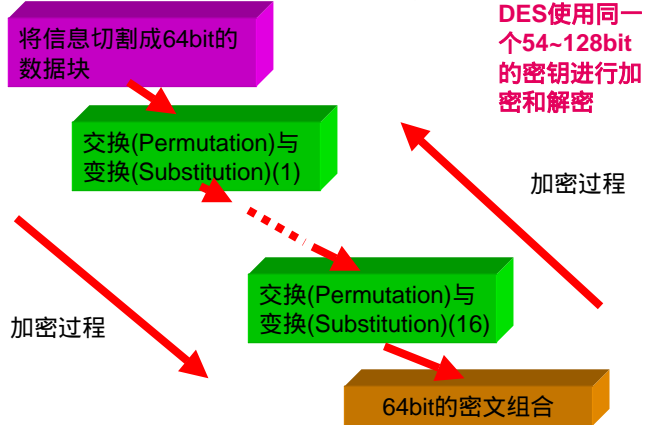
2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

24

■ 3.私钥（对称式——Symmetric Encryption）加密算法

数据加密标准DES(Data Encryption Standard)算法是由美国IBM公司研制的一种分组密码算法，于1977年被美国定为联邦信息标准—FIPS-46。是最早应用于各个领域的加密算法。



2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

25

DES加密算法的特点

■ 优点

- 速度快（相对于公钥算法）
- 易通过硬件实现
- 良好的抗破解性（迄今还未找到一种破译DES的行之有效的方法）
- 可以用三把不同的DES密钥对数据连续加密三次，构成Triple-DES，等价于将DES的密钥长度增加到112位。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

26



DES加密算法的特点

- 缺点
 - 加密密钥与解密密钥相同。
 - 密钥的传送（缺乏安全手段），即要求提供一条（假设的）安全通道使通讯双方在首次通讯时协商一个共同的密钥。
 - 由于每一对的通讯均需要使用不同的密钥而使密钥的数目将快速增长而变得难于管理；n个用户的网络，需要 $n(n-1)/2$ 个密钥，当n较大时怎么办？通信双方要经常更换密钥。
 - 一般不提供信息完整性的鉴别；不适合用于身份认证、消息真伪辨别、数字签名等。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

27



■ 4.公钥（非对称式——Asymmetric Encryption）加密技术

目前最著名的公钥密码体制就是RSA体制，它是由美国MIT的三位科学家Rivest，Shamir和Adleman提出的。

- **设计密钥：**
先仔细选取两个互异的大素数P和Q，令：

$$r : P \times Q$$

$$z : (P-1) \times (Q-1)$$
 接着寻求两个正整数d和e，使之分别满足：

$$\gcd(d, z)=1, e \times d \equiv 1 \pmod{z}.$$
 这里： (e, r) 为可公开的加密密钥， (d, r) 为保密的解密密钥。
- **设计密文：**
把要求发送的明文信息M数字化分块：

$$C \equiv M^e \pmod{r}$$
 这里C为密文。
- **恢复明文：**
对C解密，即得到明文：

$$M \equiv C^d \pmod{r}$$

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

28



RSA算法的安全性

■ 大整数分解发展状况：

年度	被分解长度（位）	时间	机器形式
1983	47	3天	HP小型机
1983	69	32小时	Cray
1988	90	几星期	25个SUN WS
1989	95	1个月	1MZP CPU
1989	106	几个星期	80个 WS
1993	110	1个月	128x128CPU
1994	129	8个月	1600部电脑

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

29



RSA算法的安全性

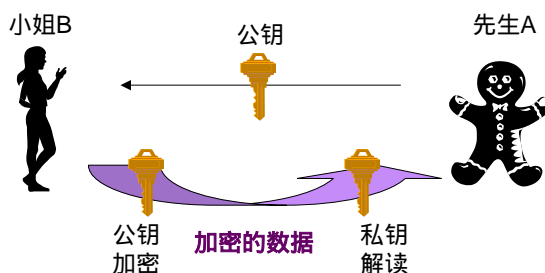
- 1996年，129（43个国家，600多人，1600台主机，分解出64和65 位两个因子，原来估计4亿亿年），1996年10月130位被用筛选法分解出。
- RSA算法需要使用足够大的整数：
512bit（154位），664bit（200位），1024bit等已有实用产品。
- 估计：100万次/s分解664bit的大整数，需要 10^{23} 步计算，约用1000年。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

30

RSA算法的运作方式



- B要先取得A的公钥；（常见方法：将所有人的公钥均放在“目录服务器（Directory Server）”中）；
- B用A的公钥将数据加密后发送给A；
- A用自己的私钥解开接收到的经过加密的数据。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

31

RSA加密算法的应用实例——对文件加密传输的实际过程


- 发送方（通过DES）生成一个自己的私有密钥，并用接收方的公开密钥（RSA）对该私有密钥进行加密，然后通过网络传输到接收方；
- 接收方用自己的（RSA）私有密钥对其进行解密后得到发送方的私有密钥（DES）；
- 发送方对需要传输的文件用自己的私有密钥（DES）进行加密，然后通过网络将加密后的文件传输到接收方；
- 接收方用发送方的私有密钥（DES）对文件进行解密得到文件的明文形式。

即两个加密解密过程：文件本身和私有密钥。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

32



2002-3-23

■ 公钥(双钥或非对称)加密体制的特点

- 这种体制的加密密钥和解密密钥不相同，而且从其中一个很难推出另一个。
- 优点：
 - 密钥分配简单
 - 密钥的保存量少
 - 满足互不相识的人之间进行私人谈话时的保密性需求
 - 可以完成数字签名和数字鉴别

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

33




2002-3-23

■ 5.存在的问题

- 加密速度慢，如RSA与DES相比，速度慢1000—5000倍左右。
- 由于缺乏一个安全交易的通用标准，所以不同的商家可能会采用不同的标准。
- 由于加密技术是国家控制的技术，很多加密技术的出口自然受到美国国家安全局的限制。

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

34



■ 4.2.2 身份认证

1. 数字签名(Digital Signature)


即可以代表“签名者”与被签名的“文件”之间关联性的“数字代号”。

- 数字签名必须保证
 - 接收者能够核实发送者对报文的签名
 - 发送者事后不能抵赖对报文的签名
 - 接收者不能伪造对报文的签名
- 当接收方收到发送方发来的签名文件后，要做两件事
 - 该签名是否为发送方的“亲笔签名”？若是，则
 - 确认文件在传输过程中有无被他人篡改过？

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

35



注意：

- 数字签名的目的是用来识别资料来源，本身并不具备对资料进行加密的功能；即被签过名的文件是以明文方式传送。若需要对文件签名的同时又希望对文件的加密，则需配合其它的加密算法。
- 注意：数字签名无法通过对称式加密法来实现，而一般是通过非对称式加密法的反向运作来实现。

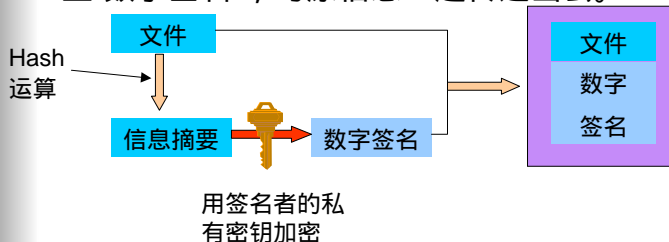
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

36

如何“签名”

- 每人自己先生成一组非对称密钥，并将加密用的密钥作为私有密钥自己保留，而将另一个密钥作为公有密钥放在公开的地方让他人存取；
- 对文件签名时，先将文件通过Hash函数运算生成一份“信息摘要”（Message Digest）；
- 将该信息摘要与签名者的私有密钥作运算，产生“数字签名”，与原信息一起传送出去。



用签名者的私有密钥加密

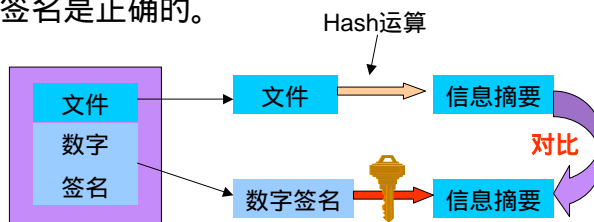
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

37

如何解读“签名”的文件

- 文件接收者在收到该签名文件后作反向运作，即将信息原文通过Hash函数运算产生“信息摘要”；
- 用签名者公布的公钥解开数字签名取得其中的信息摘要，两者做比较，若相同则表示该签名是正确的。



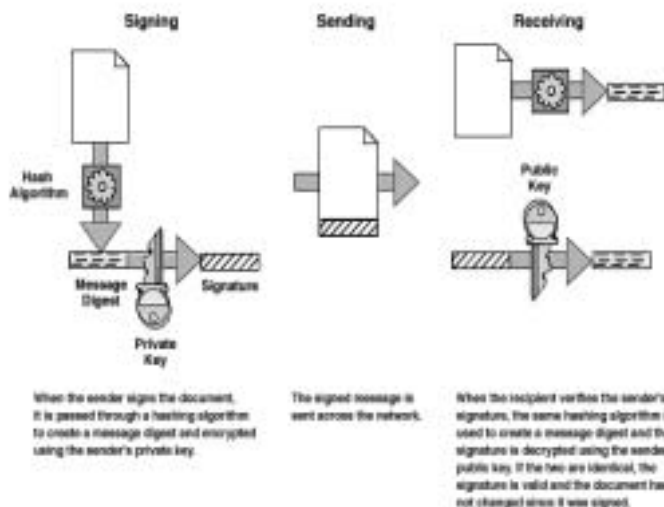
用签名者的公有密钥解密

2002-3-23

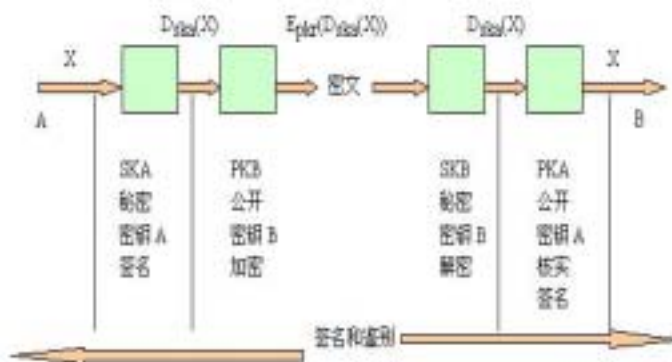
北京大学计算机科学技术系(版权所有，未经许可，不得转载)


38

数字签名运作过程



实例：具有保密性报文的数字签名过程





2002-3-23


数字签名的作用

- 若数字签名可用签名者的公开密钥正确地解开，则表示该数字签名是由签名者所产生的；
- 两者的信息摘要相同表示文件没有被他人篡改过。

■ 问题：如何证明公钥的确为某人所拥有？若无法证明则后果如何？

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

41

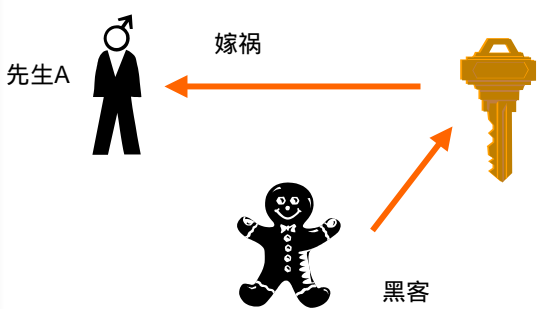


2002-3-23

数字签名的潜在问题

■ 如何证明公钥的确为某人所拥有？

例：某黑客产生一对密钥，并对外宣称该对密钥为A先生所拥有，则此黑客可以用这对密钥作坏事并嫁祸于A。




先生A

嫁祸

黑客

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

42



解决办法

- 采用数字证书，将“公钥”与其拥有者紧密结合。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

43



2.数字时间戳(Digital Time-stamp)、

是一个经加密后形成的凭证文档，它包括三个部分：

- 需加时间戳的文件的摘要(Digest)
- DTS收到文件的日期和时间
- DTS的数字签名

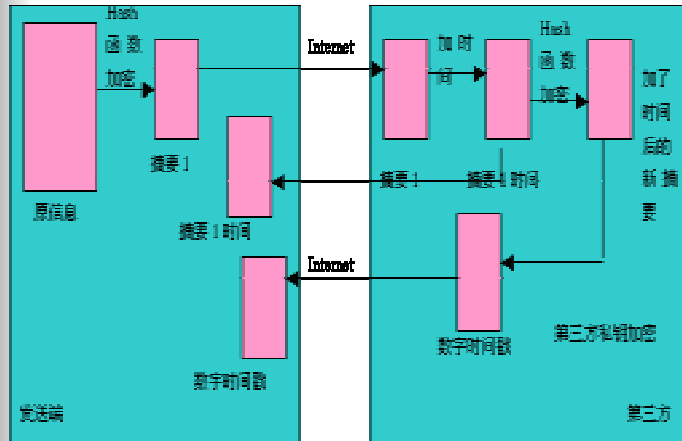
注：数字时间戳服务(DTS—Digital Time-stamp Service)

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

44

数字时间戳



2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

45

3. 数字证书(Digital Certificate)

数字证书相当于网络上的证明文件, SET和 Secure MIME等协议均以数字证书为基础。数字证书的内部格式是由CCITT X.509国际标准所规定的, 它包含了以下几点:

- 证书拥有者的姓名
- 证书拥有者的公共密钥
- 公共密钥的有效期
- 颁发数字证书的单位
- 数字证书的序列号(Serial number)
- 颁发数字证书单位的数字签名

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

46

数字证书的类型

- 个人证书(Personal Digital ID)
 - 以个人的身份识别数据（如身份证）向认证中心申请即可，常见的包括电子邮件、电子文件等。
- 企业(服务器)证书(Server ID)
 - 以公司名义申请，必须提供合法证明（如营业执照）向认证中心申请，常见的包括网络商店的识别标识等。
- 软件(开发者)证书(Developer ID)
 - 属于个人证书的一种。

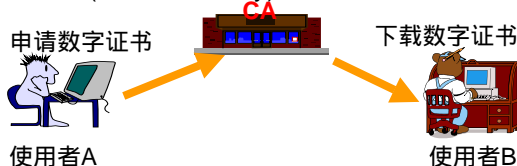
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

47

X.509 证书结构

- 版本(version)：区分X.509证书格式的的版本
- 序号(Serial Number)：识别证书的唯一编号
- 算法(Algorithm Identifier)：指认证中心用来签发该证书的公开密钥算法
- 发证者(Issuer)：核发该证书的认证中心
- 发证者识别码(Issuer Unique Identifier)
- 使用者(Subject)：拥有此公钥的使用者
- 使用者识别码(Subject Unique Identifier)：用以识别个别使用者的识别码
- 公钥信息(Public Key Information)：与使用者对应的公钥与其公开密钥算法名称
- 有效日期(Period Validity)：包括起止日期



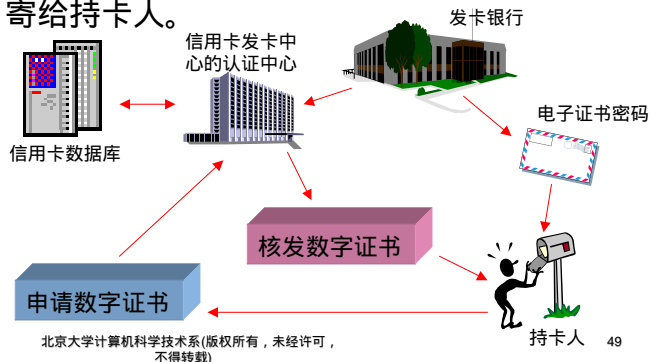
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

48

数字证书的申请方式

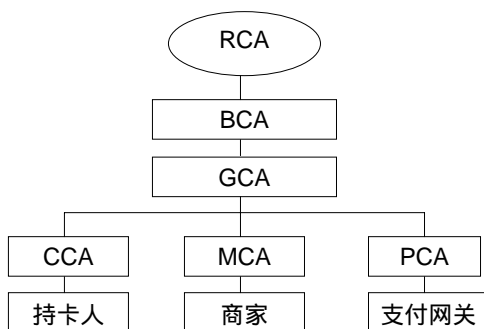
- 持卡人向发卡银行要求申请数字证书，这时发卡银行认证中心向信用卡数据库查询持卡人的数据；
- 发卡银行认证中心确认持卡人的身份无误后，即可签发数字证书给持卡人；
- 数字证书的密码等机密数据则通过信件方式寄给持卡人。



认证中心(Certificate Authority)

- 认证中心是一个独立、公正、可信赖的组织，负责证书的管理工作，包括：
 - 建立签发数字证书的原则
 - 签发数字证书（认证中心在核准申请者的数字证书后用自己的私钥签名）
 - 注销数字证书（所有注销的数字证书均列在“证书注销表（CRL——Certificate Revocation List）”中供大家查询）
 - 其他管理功能（如申请者的数据、数字证书的备份和更换等）

认证中心的结构



RCA(Root CA) : 信用卡认证结构的最高管理单位

BCA(Brand CA) : 各家信用卡公司的认证单位

GCA(Geo-Political CA) : 各家信用卡公司分支

CCA(Card Holder CA) : 负责办理持卡人数字证书的认证中心

MCA(Merchant CA) : 负责办理商家数字证书的认证中心

PCA(Payment Gateway CA) : 负责办理支付网关的数字证书的认证中心

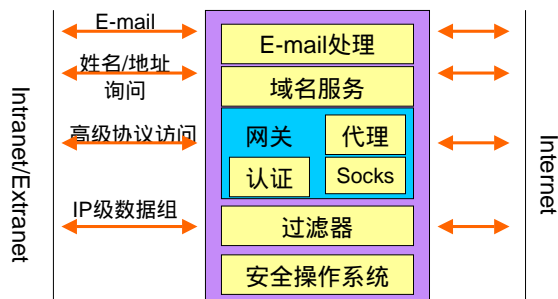
2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

51

■ 4.2.3 防火墙技术

所谓防火墙,就是在内部网与外部网之间的界面上构造一个保护层,并强制所有的连接都必须经过此保护层,在此进行检查和连接。只有被授权的通信才能通过此保护层,从而保护内部网及外部的访问。



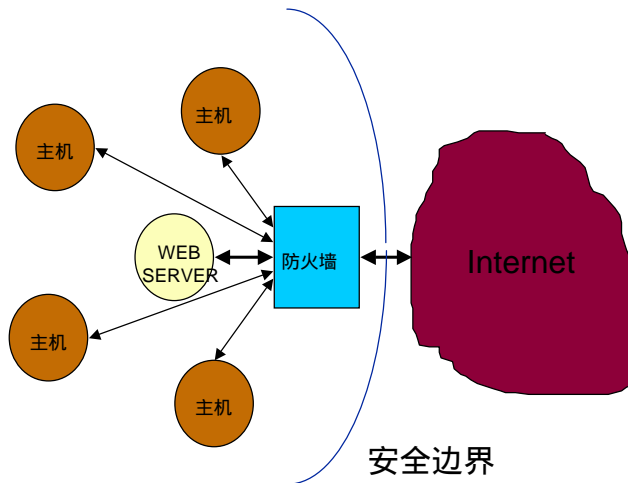
防火墙的构成

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

52

Web Server处于防火墙内

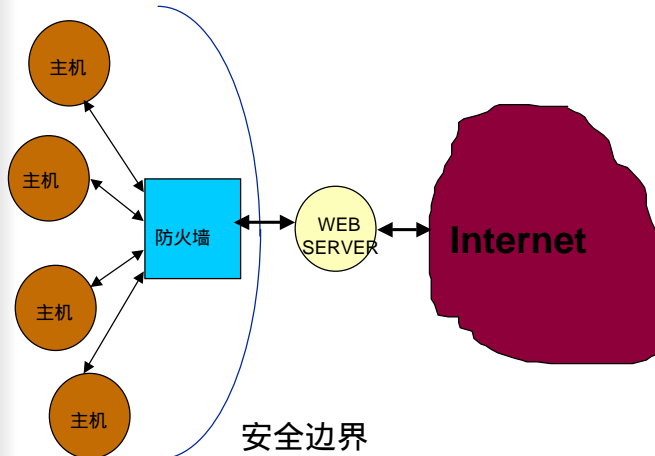


2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

53

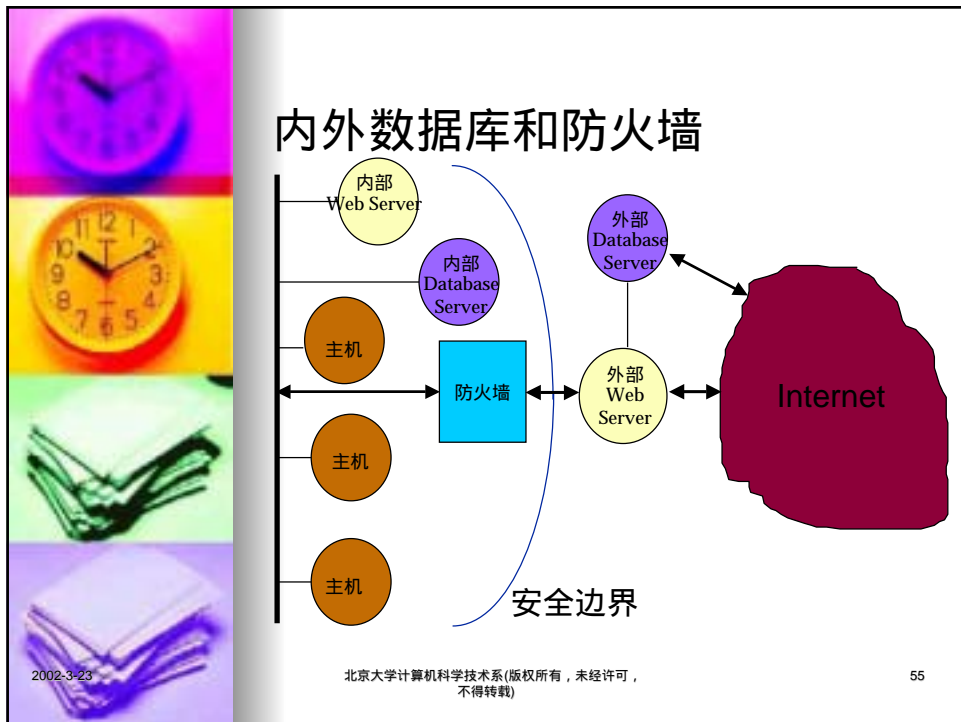
Web Server 在防火墙之外



2002-3-23

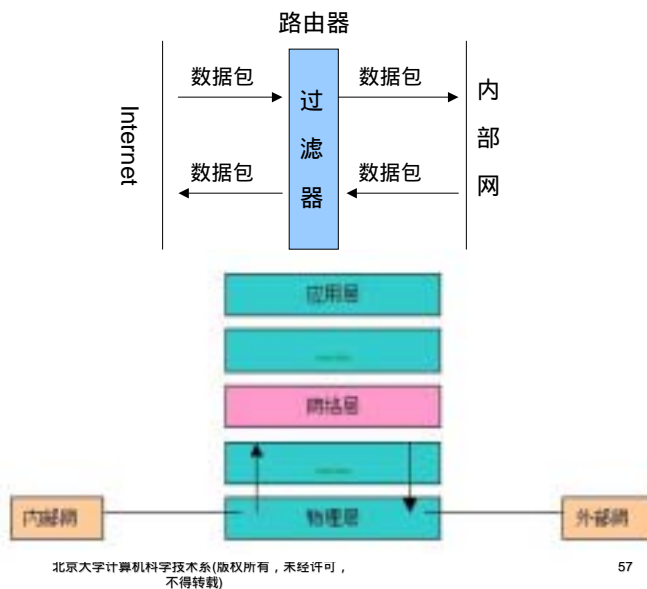
北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

54



-
- 防火墙的优点
- 保护那些易受攻击的服务
 - 控制对特殊站点的访问
 - 集中化的安全管理
 - 对网络访问进行记录和统计
- 防火墙的安全控制模型
- 没有被列为允许访问的服务都是被禁止的
 - 没有被列为禁止访问的服务都是被允许的
- 2002-3-23
- 北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)
- 56

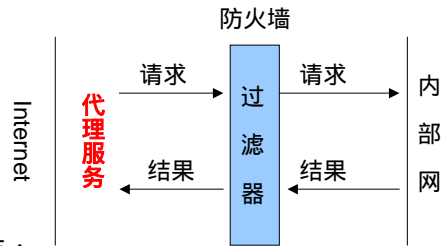
1.包过滤防火墙



■ 包过滤防火墙的特点

- 价格低, 对用户透明, 且对网络性能影响很小;
- 只对源和目的IP地址及端口检查;
- 配置复杂, 需要具备网络、数据传输方面的细节知识, 甚至协议方面的知识;
- 无用户使用记录
- 对IP欺骗式攻击 (IP Spoofing) 比较敏感。

2. 代理服务型防火墙



特点：

- 将跨越防火墙的网络通信链路分为两段

优点：

- 将被保护的内部网络结构屏蔽起来，
- 可实施较强的数据流监控、过滤、记录和报告

缺点：

- 需为每个网络服务专门设计、开发代理服务软件及相应的监控过滤功能
- 代理服务器需专门的工作站承担
- 速度较慢

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

59

3. 复合型防火墙

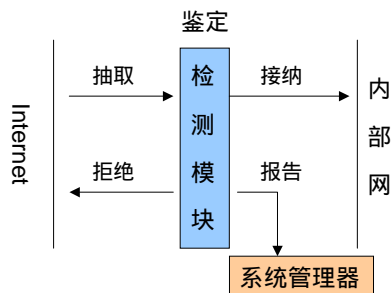
这种防火墙是把前两类防火墙结合起来，形成新的产品，以发挥各自的优点，克服各自的缺点，来满足更高安全性的要求。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

60

4. 状态监视器防火墙



■ 优点：

- 安全特性非常好
- 检测模块采用抽取相关数据的方法对网络通信的各层实施监测，同时对抽取的部分数据即状态信息加以保留以便作为今后制定安全决策的参考
- 检测模块支持多种协议和应用程序，并具有可扩充性
- 检测模块监测RPC和UDP之类的端口信息

■ 缺点：

- 配置复杂，速度较低

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

61

防火墙的安全业务

■ 用户认证

- 针对防火墙用户和管理员

■ 域名服务：

- 提供对外及内的可访问主机IP地址

■ 邮件处理

- 采用SMTP(Simple Mail Transfer Protocol)，检验邮件的合法性

■ IP的安全性

- 包含两层，即认证和保密

■ 防火墙IP的安全性

- 提供保密性和完整性

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

62

防火墙的安全体系

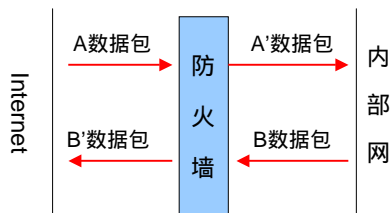
1. 双重宿主主机体系

- 至少有两个网络接口，主机可以充当网络之间的路由器，但关闭路由；
- 防火墙内外的网络系统均与双重宿主主机通信，内外之间不直接相连（即将双方的IP通信完全隔断）。
- 类似海关，但双重宿主主机要仔细检查数据包的内容并将其改头换面重新包装；
- 在双重宿主主机上有内外数据的缓冲区。

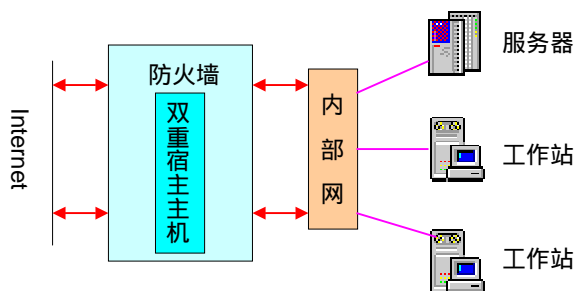
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

63



双重宿主主机通信原理图



双重宿主主机体系结构

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

64

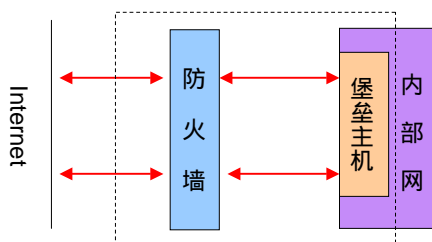
2. 屏蔽主机体系

- 使用一个单独的路由器提供来自与内部的网络相连的主机服务；
- 通过防火墙和内部网络上的堡垒主机（Bastion Host）完成数据包过滤
- 其防火墙是由路由器和堡垒主机组成；
- 路由器上的数据包过滤可以是：
 - 允许其内部主机为了某些服务与Internet上的主机连接（即允许那些已经由数据包过滤过的服务），或
 - 不允许来自内部主机的所有连接（即强迫那些主机经由堡垒主机使用代理服务）
- 该体系比双重宿主主机体系具有更高的安全性和可用性。
- 缺点是：堡垒主机易成为诱人的攻击目标。

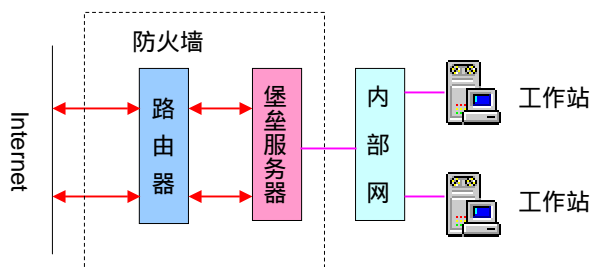
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

65



屏蔽主机体系原理图



屏蔽主机体系

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

66

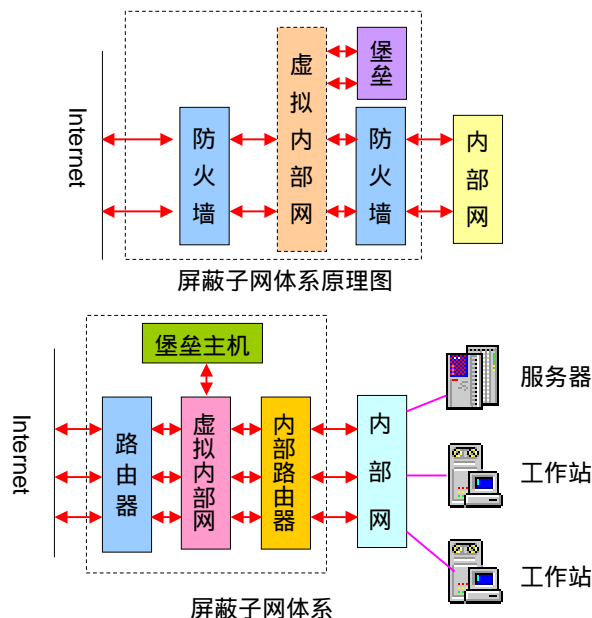
3. 屏蔽子网体系

- 针对屏蔽主机体系中堡垒主机易受攻击的弱点，在被屏蔽的主机体系中增加额外的安全层——虚拟的内部网，进一步将内部网与Internet隔开；
- 防火墙为两个屏蔽路由器，一个位于虚拟内部网与内部网之间，一个位于虚拟内部网与Internet之间；
- 即使侵袭者突破了第一道防火墙，他所看到的是个虚拟的内部网和堡垒主机，并无实质东西可利用，而稍有“不慎”即可露出“马脚”；
- 不存在内部网络的单一易受侵袭点。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

67



2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

68




防火墙的设计

- 防火墙的功能
 - 拒绝没有特别允许的任何事情（即假定应该阻塞所有信息，缺点是不易使用）
 - 允许没有特别拒绝的任何事情（即假定应该转发所有信息，缺点是将易用性放在了安全性前面）
- 机构的整体安全策略
 - 保护对象，安全分析，风险评估，商业需求分析
- 防火墙的费用
 - 商业的防火墙为\$4000~30000
 - 维护管理、升级、补漏、事故处理等
- 防火墙的构件
 - 包过滤路由器（对每个包进行检查确定可否接收）
 - 应用层网关（或代理服务器，对服务进行控制）
 - 电路层网关（只依赖TCP连接，不进行包过滤）

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

69



4.3 电子商务安全交易标准

- 4.3.1 安全超文本传输协议（S-HTTP）

安全超文本传输协议(S-HTTP)用密钥对来加密，以保障Web站点上的信息的安全。为Web文档提供安全和鉴别，保证数据的安全。

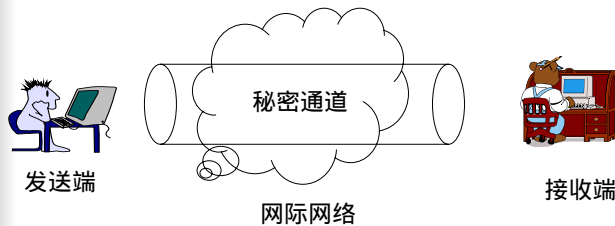
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

70

■ 4.3.2安全套接口协议（SSL）

安全套接层协议（SSL——Secure Socket Layer）则保证了Web站点之间通信信道的安全，对面向网络协议栈的低层通道进行安全监控。



2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

71

SSL提供的安全防护

- 由Netscape在1995年6月发表，目前为3.0版；
- 可对TCP/IP以上的网络应用协议数据流加密，如HTTP、TELNET、FTP等；
- 结合密码学的技术，如信息加解密、数字签名和签证技术等；
- 采用了公开密钥和私钥两种加密方式：
 - 在建立连接过程中采用公开密钥，通过“握手”（handshaking）方式建立连接；
 - 在会话过程中使用专有密钥

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

72



SSL提供的三种安全防护

- 数据的机密性与完整性
 - 通过数据的加解密实现
- 服务器的个体识别服务
 - 利用服务器的数字证书来验证商家的资格
- 客户端的个体识别服务
 - 通过客户端自己的数字证书来完成

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

73



SSL协议原理

- 包含两个协议
 - SSL Handshake
 - SSL Record

HTTP	FTP	SMTP
Secure Socket Layer		
TCP		
IP		

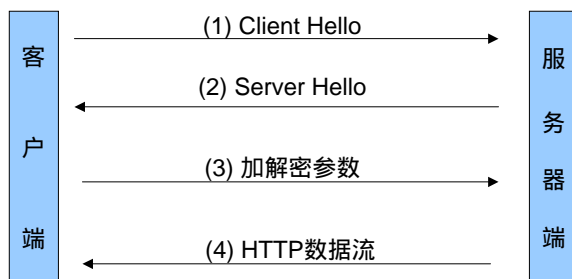
2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

74

SSL Handshake 协议

- SSL版本
- 信息加密用的算法
- 客户端身份验证要求
- 所使用的公开密钥算法

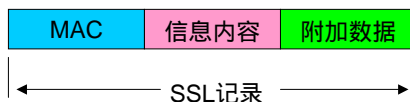


2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

75

SSL Record协议



- MAC(Message Authentication Code)：固定长度，用于验证信息内容是否完整的验证码，由Hash函数完成
- 信息内容：指应用层传来的数据，如HTTP信息
- 附加数据：指加密后产生的附加信息

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

76



支持SSL的服务器和浏览器

- Netscape Communicator 2.0以上
- Microsoft Internet Explorer 3.0以上
Web服务器Microsoft IIS
- Apache Freeware
- Lotus Notes Server 4.1
- Lotus Domino Server 4.5
- Open Market

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

77



S/MIME中对电子邮件采用的对称加密方法

- DES——(Data Encryption Standard)
- Triple DES : 即三次DES
- RC2 : 密钥的长度可以伸缩 (以便符合密码出口的限制)

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

78




S/MIME的特色

- 可扩充性
 - 相对于PGP(Pretty Good Privacy——用于局域网，人数有限)
 - 采用层次结构，因此适用范围可小至局域网，大至Internet。
- 使用业界标准
 - 信息格式：继承MIME规格
 - 信息加解密标准：KCS(Public Key Crypto System Standard)
 - 数字证书格式：X.509 Certificate
- 开放性结构
 - 支持S/MIME标准的任何软件均可互通

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

79



4.3.4 UN/EDIFACT的安全


UN/EDIFACT报文是唯一的国际通用的EDI标准。

UN/EDIFACT的安全措施主要是通过集成式和分离式两种途径来实现。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

80




■ 4.3.5安全电子交易规范（SET）

- 由Visa、MasterCard共同推出，并与Microsoft、Netscape、RSA等公司共同发展而成，1996年2月1日发表。目前已经标准化。
- SET是向基于信用卡进行电子化交易的应用提供了实现安全措施的标准或规则。
- SET使用的加密技术
 - 密钥系统
 - 公钥系统
 - 数字信封
 - 数字签名
 - 双重签名

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

81



网上信用卡交易的安全需求

- 商家希望能够通过一套简单又符合实际经济效益的方式来进行网上交易；
- 客户们希望能有一套安全方便的服务，使他们可以放心地到网络上进行购物；
- 银行及信用卡机构寻求（对现有系统而言）以最小的改变就可以在未来支持电子付款的方式。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

82

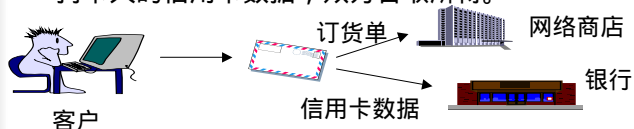
SET的起源

■ 问题所在

- 在SET未发展之前，大部分网上购物均采用SSL协议，将信用卡号加密后发给商家：
- 信用卡的相关数据应该只有银行才能看到，商家不应知道这些“私人”信息
- 存在被人盗用的条件

■ 设计目的

- 确保整个交易过程中每个节点所传送的数据的安全性
- 确保订单及付款数据不被他人所篡改
- 确认商家与持卡人双方身份不为假冒
- 商家只可看到持卡人的订购数据，银行只能取得持卡人的信用卡数据，双方各取所得。



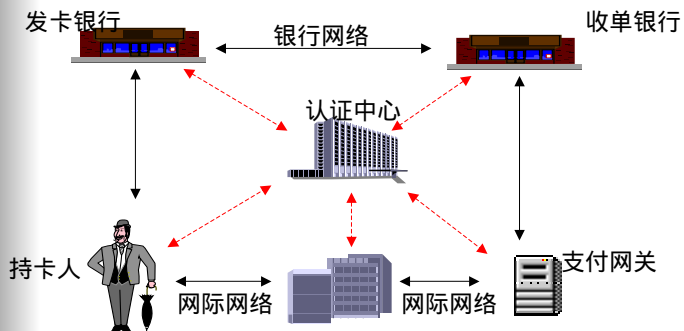
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

83

参与SET的交易成员

- 持卡人
- 商家
- 发卡银行
- 收单银行
- 认证中心
- 支付网关

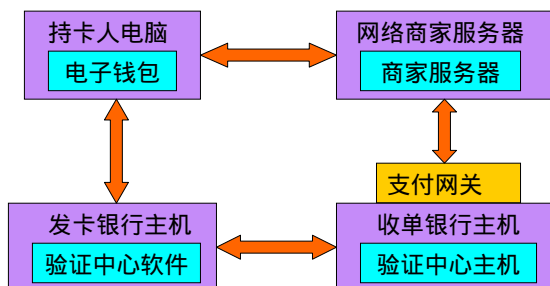


2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

84

SET软件的组件

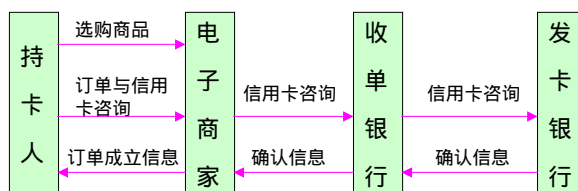


2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

85

SET的运作流程



1. A先生进入网络商家订购书籍, 并填写订购数量、送货日期等信息;
2. A先生准备结帐, 这时计算机中具有SET规格的“电子钱包”软件自动启动, 并将信用卡信息连同订单信息分别加密后传送给商家;
3. 商家B收到该订单及信用卡信息后, 将信用卡信息原封不动的传给收单银行, 以检查信用卡是否有效;
4. 收单银行向发卡银行确认该信用卡数据无误后, 发出信息通知商家可以接下此笔订单;
5. 到了结帐日, A先生会接到发卡银行的信用帐单, 而商家则可以拿信用卡授权码向收单银行划款。

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

86

SET与SSL机制的比较

- 认证机制：SET要求所有参与交易各方均必须先申请数字证书以识别身份，而SSL只有商家的服务器需要认证，客户端的认证是可选的（optional）；
- 设置成本：希望申请SET交易者除必须申请数字证书之外，也必须在计算机上安装符合SET规格的电子钱包软件，而SSL交易无须另外安装软件；
- 安全性：SET的安全性比SSL高，SSL的安全范围只限于持卡人到商家的信息交换；
- 目前采用率：SET的成本较高，目前SSL的普及率较高。

比较项目	SET	SSL
认证机制	所有参与SET的成员	商家服务器
设置成本	较高	较低
安全性	较高	较低
采用比率	约 1 5 %	约 8 0 %

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

87

4.4 黑客攻击防范措施


■ 4.4.1 黑客介绍

- “黑客”一词来源于英语动词：Hack
- 60、70年代，“黑客”(Hacker)在当时用来形容独立思考、然而却奉公守法的计算机迷。
- 今天，“黑客”意味着那些偷偷地、未经许可就打入别人计算机系统的计算机罪犯。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

88



■ 4.4.2 严峻的黑客现实

- 据统计，几乎每20s全球就发生一起黑客事件发生，仅美国每年所造成的经济损失就超过100亿美元。
- 网络是他们攻击的主要目标。
- 想有效防止黑客的入侵实在不是一件容易的事

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

89



■ 黑客的攻击手段

- 中断(Interrupt，攻击系统的可用性)
- 窃听(Sniffer，攻击系统的机密性)
- 篡改(Tamper，攻击系统的完整性)
- 伪造(Falsification，攻击系统的真实性)
- 利用网络协议的一些漏洞，获取系统的口令文件
- 对口令进行破译
- 用破译后的帐号进入系统，开始任意胡作非为
- 使用许多工具获得特权


■ 黑客的攻击方法

- 窃听网络封包 (Sniffer)
- 电子邮件攻击法 (Email Attack)
- 网络档案系统攻击 (Network File System Attack)
- 网络封包窃听与假冒攻击 (IP Spoofing)
- 拒绝服务 (Denial of Service)

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

90




2002-3-23

■ 4.4.3 黑客攻击手段

- 利用网络协议的一些漏洞，获取系统的口令文件
- 对口令进行破译
- 用破译后的帐号进入系统
- 使用许多工具获得特权
- 开始任意胡作非为

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

91




2002-3-23

■ 4.4.9 对付黑客攻击破坏的手段

- 使用防火墙
- 使用安全扫描工具发现黑客
- 使用有效的监控手段抓住入侵者
- 时常备份系统，若被攻击可及时修复
- 加强防范意识，防止攻击

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

92



思考题

1. 阐述网络安全体系结构。
2. 网络信息安全的基本要求是什么？
3. 公钥密码体制特点是什么？
4. 数字证书有什么作用？
5. 防火墙可以分为哪些类？
6. SET使用的加密技术

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

93



OVER Ch4

Thank You