电子商务

2009年复旦大学精品课程 上海市教委重点建设课程

电子商务安全
The Security in e-Commerce

戴伟辉 博士

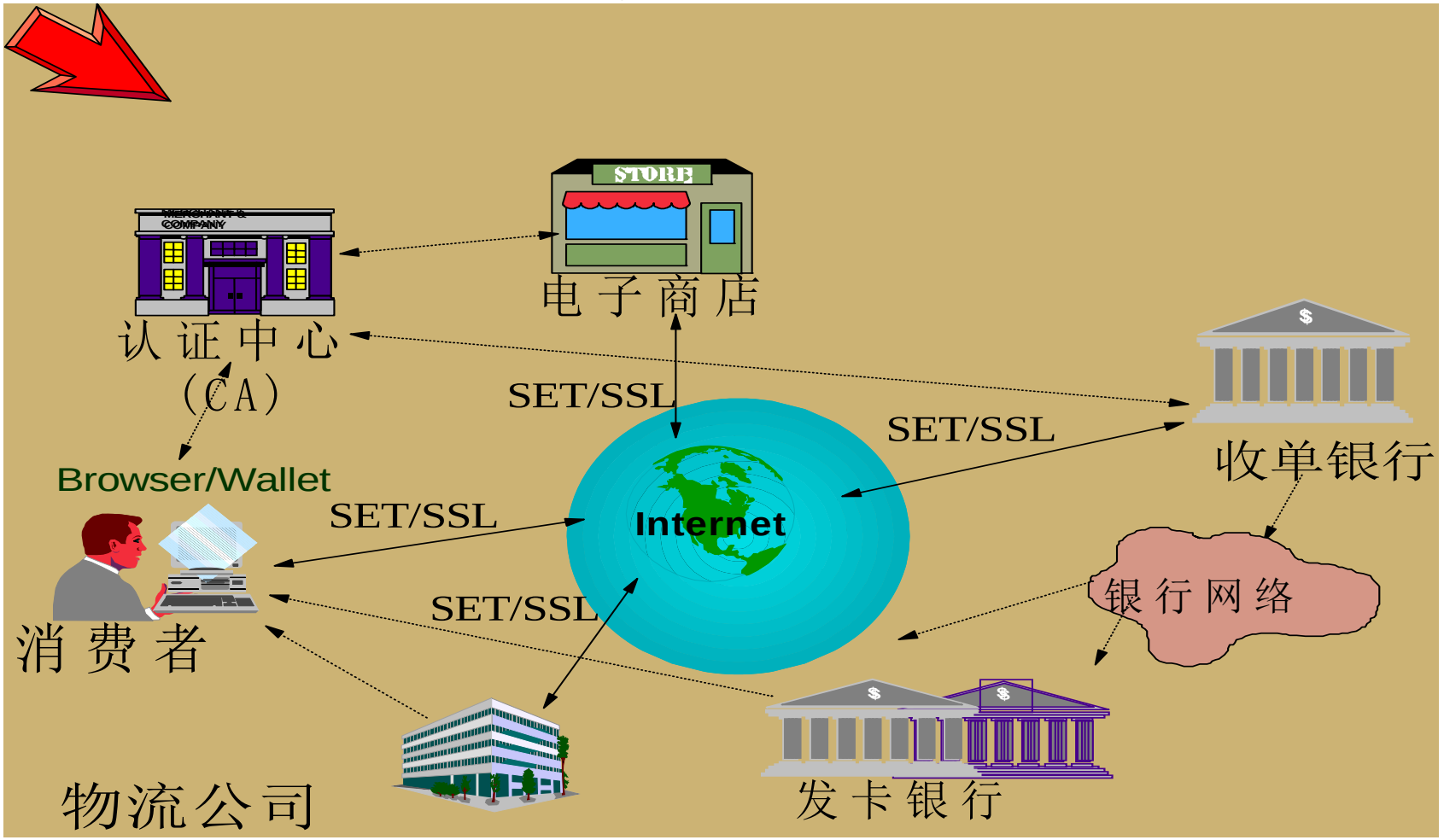
复旦大学管理学院

ebusiness FUDAN UNIVERSITY

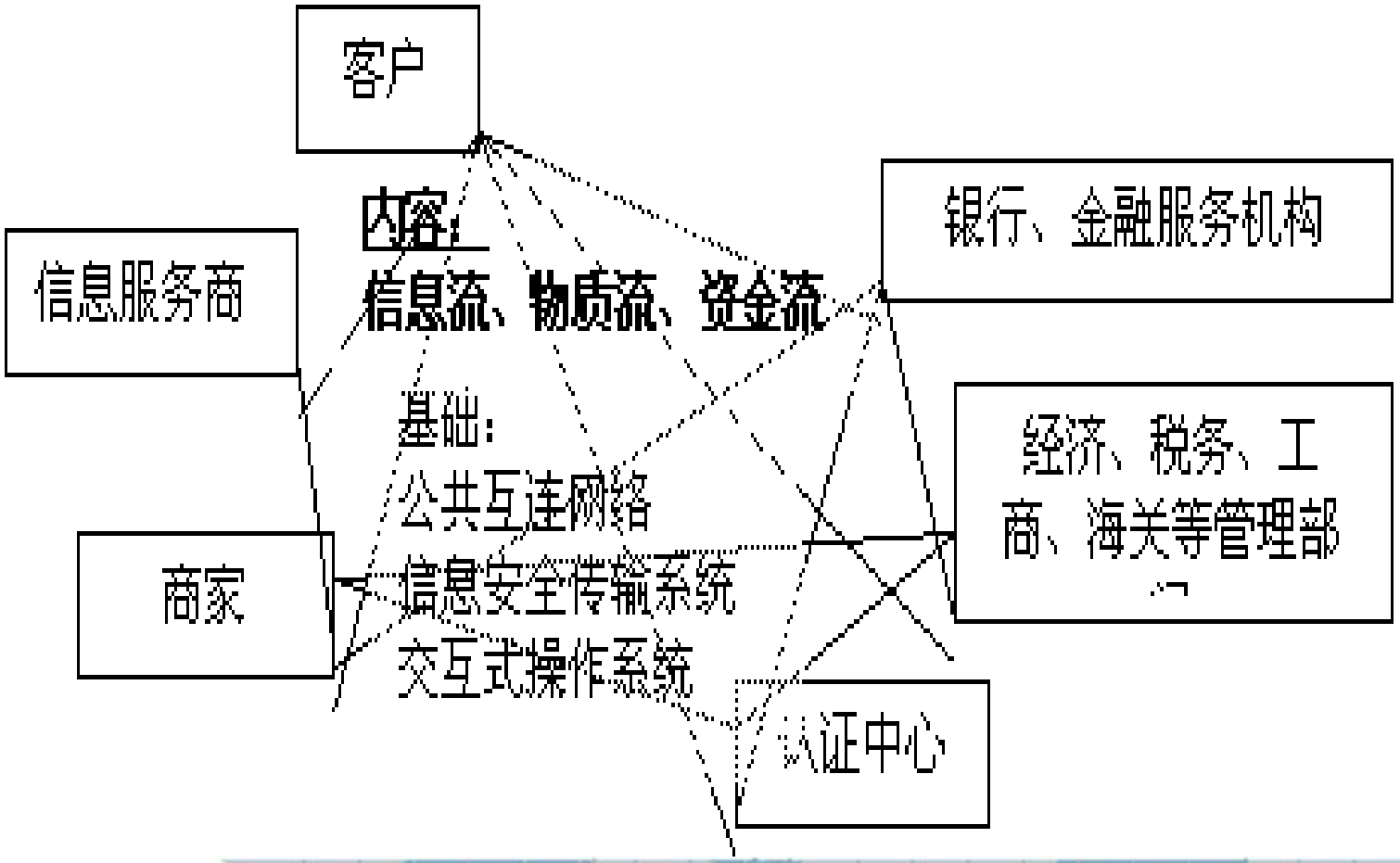
议程

- 电子商务安全问题
- 防火墙与加密技术
- 网络安全系统设计
- 研讨题：拇指花运营系统安全分析

电子商务的交易过程


STORE
电子商店
认证中心
(CA)
SET/SSL
SET/SSL
收单银行
Browser/Wallet
SET/SSL
Internet
SET/SSL
银行网络
消费者
物流公司
发卡银行

电子商务交易中的相关主体



电子商务安全问题的产生

一、交易主体：
- 电子商店；
- 网上银行；
- 消费者；
- 其它。

二、通讯过程：
- 通讯线路；
- 支付过程；
- 信息交互内容。

三、设备管理
- 银行卡；
- 上网终端；
- **Web**服务器；
- 其它网络设备。

电子商务中各方的义务

- 1）认证中心：发布用户认证证书、管理认证证书、保证认证的安全可靠，其本身必须满足管理、操作于系统的有关要求。
  - 对参与者进行严格的审查和认证
  - 保证发放的证书具有可靠的权威性和信任度
  - 发布可靠及时的认证信息
- 2）认证用户（商家、消费者等）：合法使用认证机制、获得证书，开展电子商务活动。
  - 报出本身准确的相关信息
  - 及时检查证书内容和信息
  - 妥善包管好私人密钥
  - 及时汇报出现的问题，例如密钥泄露、交易异常等现象
- 3）参与者（银行等其他相关方）：合法使用认证机制，按照有关规定进行电子商务操作。
  - 检查证书本身的合法有效性、进行证书失效检查
  - 通过其他方法确认证书的可靠性、保证业务24小时正常运行

安全报告

- **FBI**统计：每年因信息安全损失**75**亿；
- 美国金融时报：每**20**秒发生一次**Internet**入侵事件。

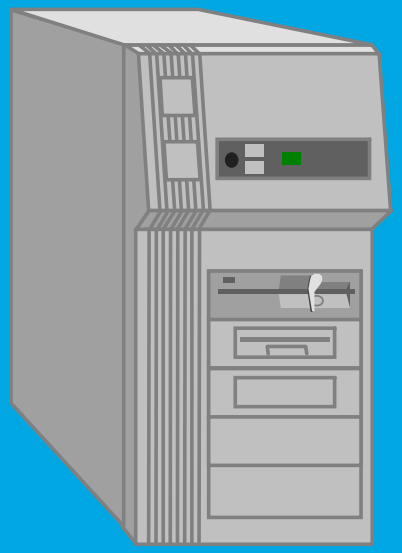
变鹿为马

互联网的公式:

计算机 + 高价值的在线交易 + 开放的互联网 + 不道德的人们

= 无限的欺诈机会

Internet 间谍



Web Server

正常连接

信息

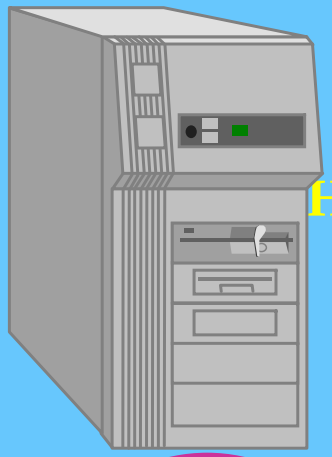
安全

ID：DAI
Password：1966

ID：DAI
Password：1966

Internet Spy

假冒 Web站点

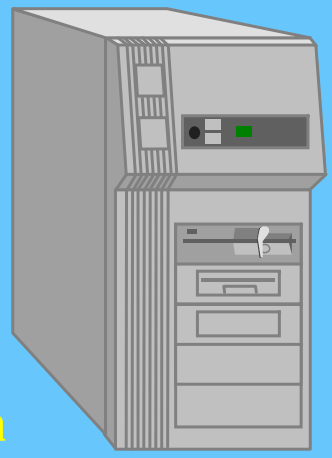


Website A
Http:// www.aaa.com

安全

Website B
假冒 www.aaa.com

当假冒服务器出现时

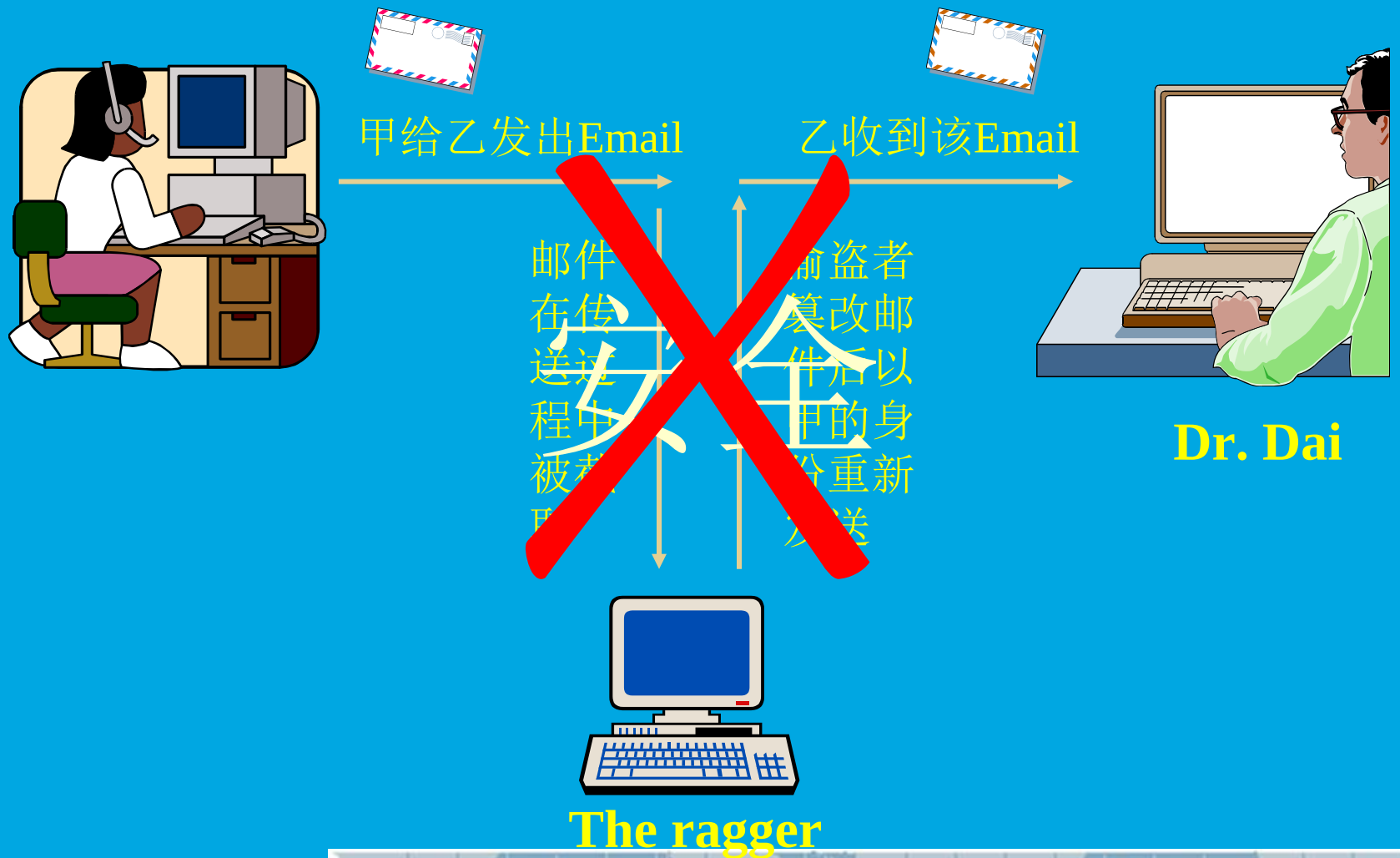


浏览者与服务器B连接，访问站点
www.aaa.com

When you want to access Website A and enter: http://www.aaa.com.
In fact, you have been linked to a disguised website B, then your ID and password maybe stolen by the webmaster of B.

ebusiness
FUDAN UNIVERSITY

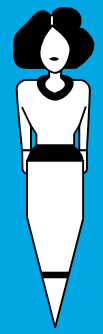
不安全的 Email


甲给乙发出Email
乙收到该Email
邮件在传送过程中被截
篡改邮件后以甲的身份重新发送
不安全
Dr. Dai
The ragger

抵赖

I want a TV Set, please sent it to my home where is :No.220 Handan Road.

甲：认发送过

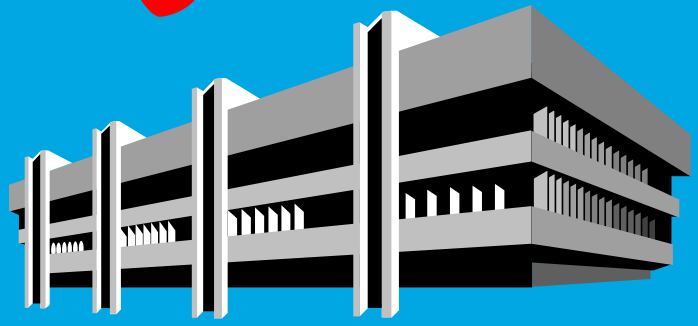


安全

商家：认收到过

来自甲的购款

No, I have never bought a TV Set.

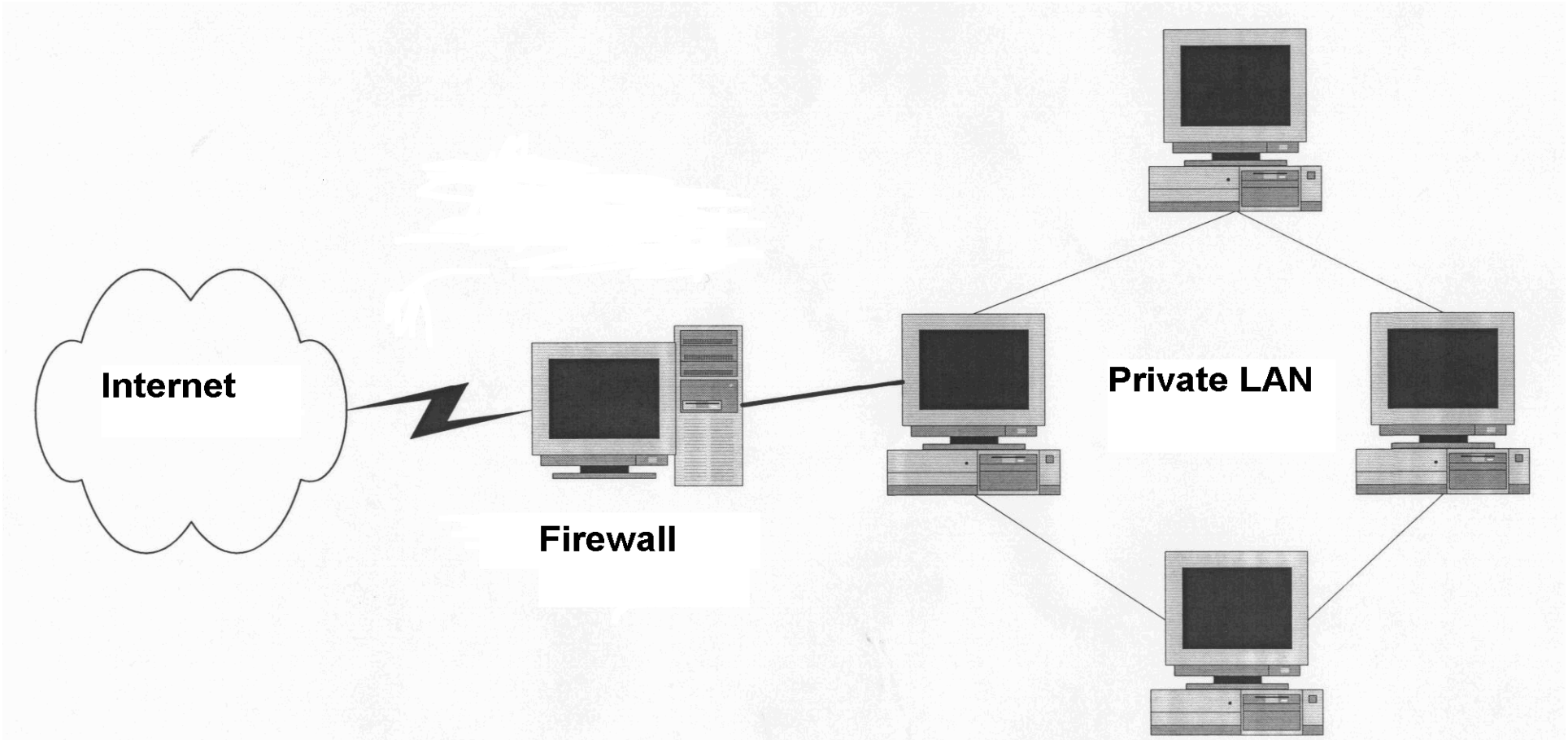


可信任的网络环境

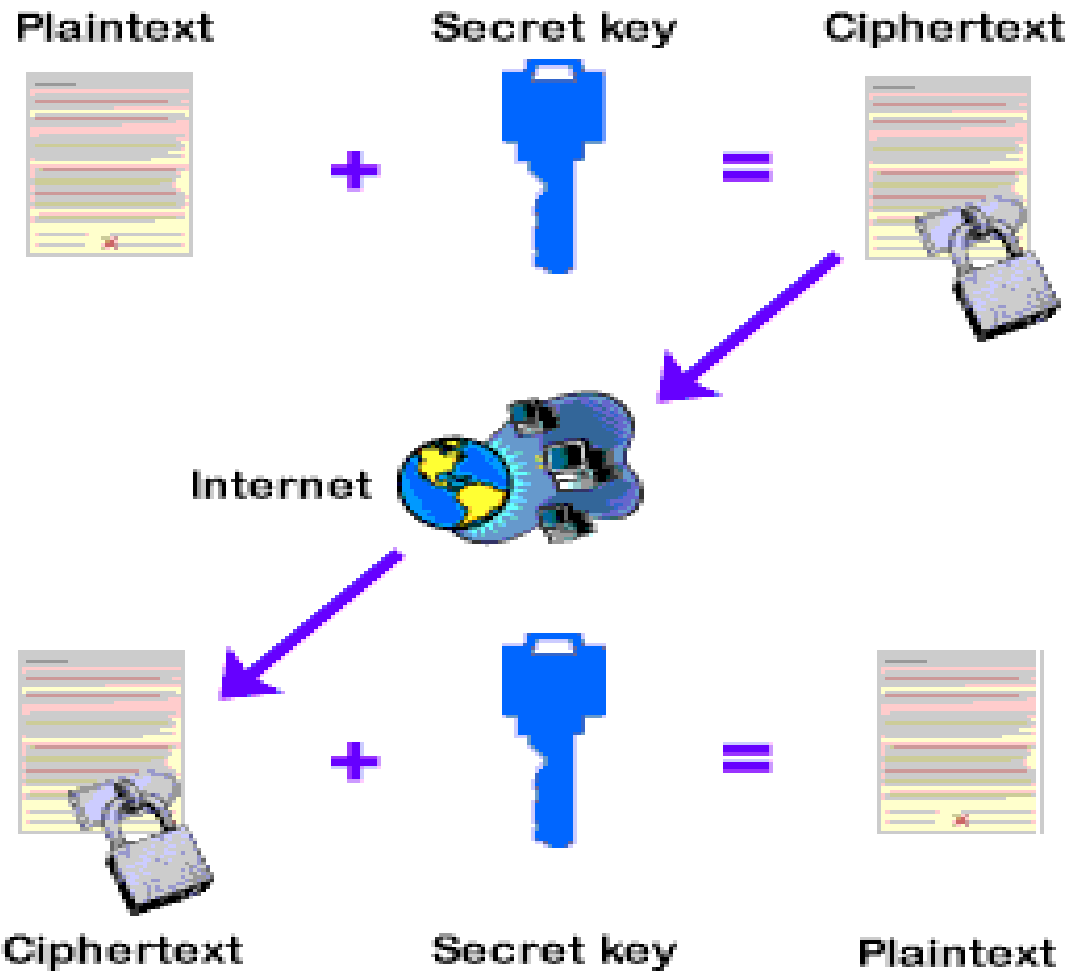
可以满足信任环境建设的上述基本要求
（公开的加密算法、加密技术和机制）

- 私有性
- 身份的真实性
- 信息的完整性
- 不可抵赖性

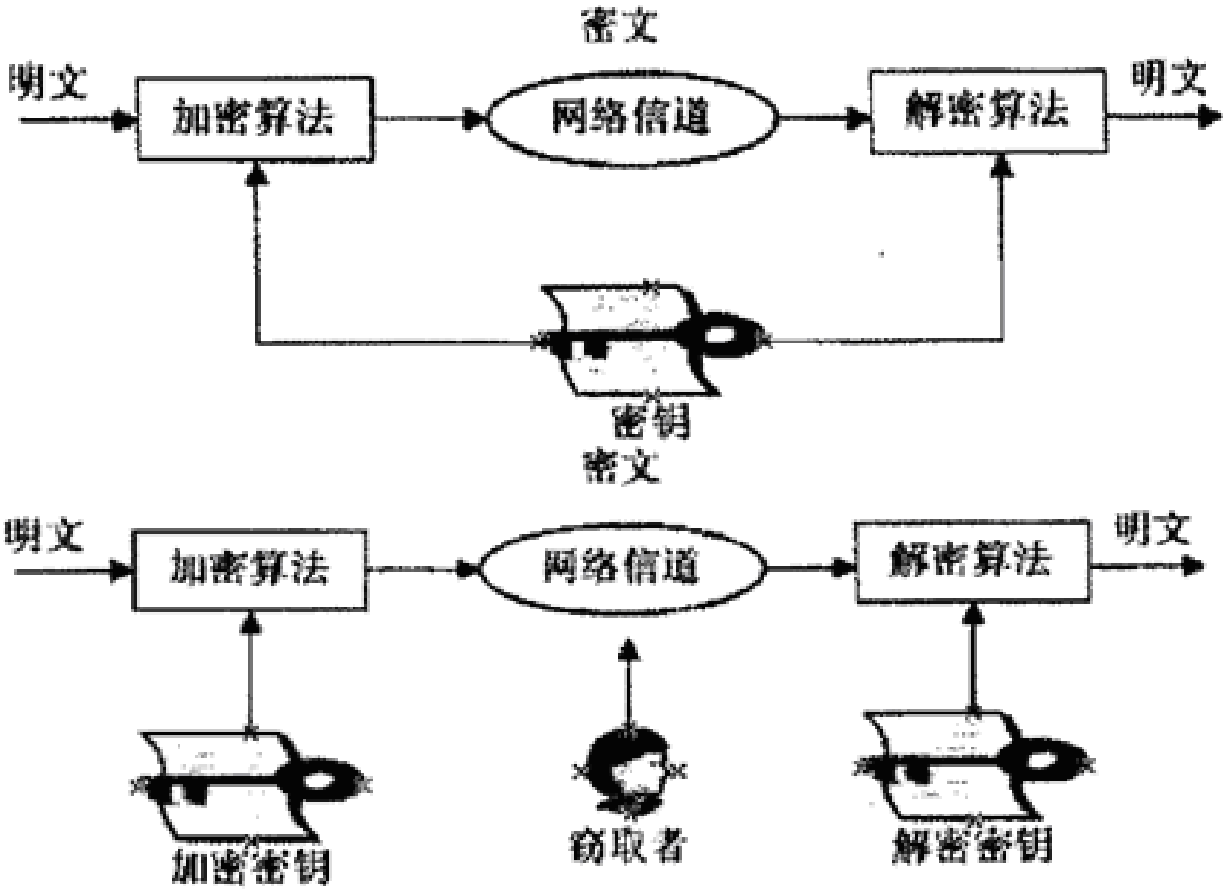
如何解决安全问题:
防火墙



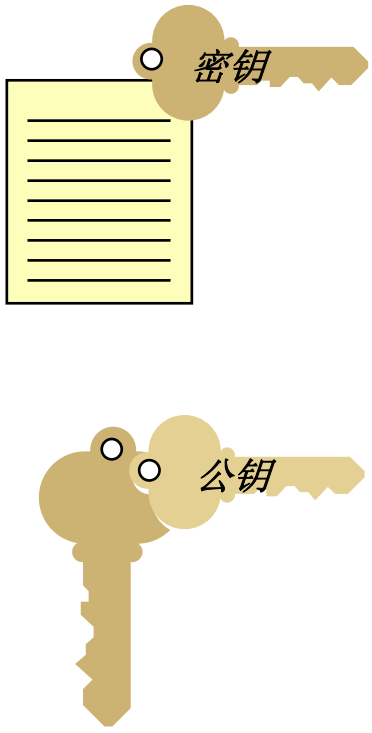
加密与解密


Plaintext
Secret key
Ciphertext
Internet
Ciphertext
Secret key
Plaintext

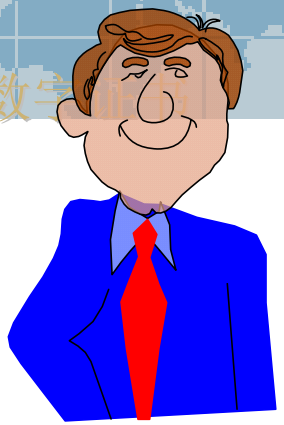
对称加密与非对称加密



应用于电子商务安全的两种加密技术

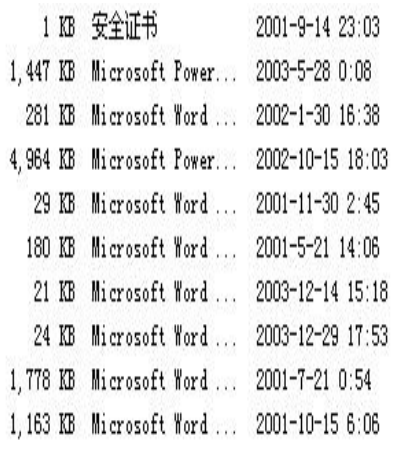


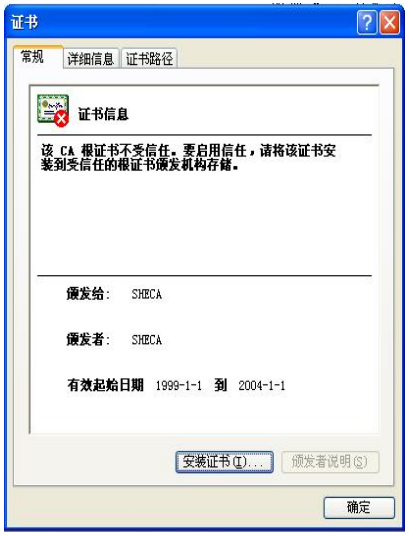
- 数字信封
  发送方产生随机对称密码，将传送的信息用该对称密码加密，该对称密码用接收方的公钥加密，一同发送给接收方。
- 数字签名
  比真实的签名更具有不可伪造性。数字签名是一段数据，与发送的数据相关，并用自己私钥加密，发送的数据一旦更改，数据签名肯定更改，并没有第二个人可以作出同样的签名。

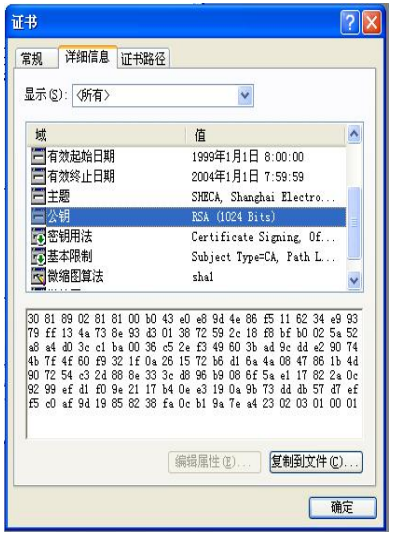


好游先生

- CA 数据库给每一位用户登记一个唯一的证书电子标识
- 电子标识
  - 以保护格式存储
  - 通过使用用户口令进行合法操作
  - 或采用 PCMCIA令牌卡，高安全级别







磁盘介质存储

IC卡介质存储

ebusiness
FUDAN UNIVERSITY

第三方信任的模型

证书信任机构举例

公安局(身份证、护照、驾驶证)

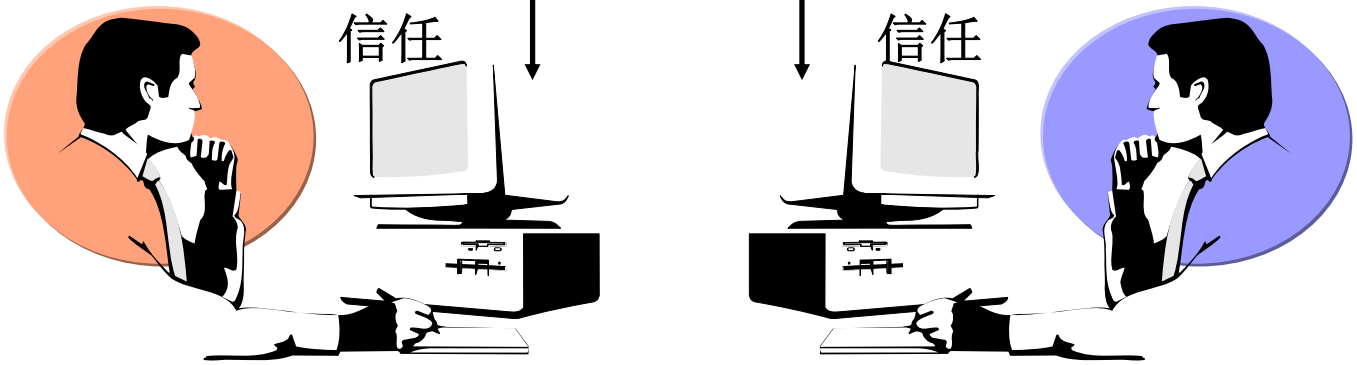
院校（毕业文凭）

银行 （信用卡）

CA（证书认证中心）

互相信任

互相信任



第三方信任

证书类型

- 个人身份证书：该类证书证明客户的公钥和身份。在某些场合，如建立SSL连接或交易服务时， 服务器可能需要客户端的证书
- 企业身份证书 ：该类证书证明企业的公钥和身份。在某些场合，如建立SSL连接或交易服务时， 服务器可能需要客户端的证书
- 服务器身份证书：该类证书证明服务器的身份和公钥。在与客户端建立SSL连接的场合，服务器将它的证书发给客户
- CA证书： 证书认证中心签名密钥的证书。
- 软件代码证书：对软件进行签名
- 信用卡身份证书：符合SET协议

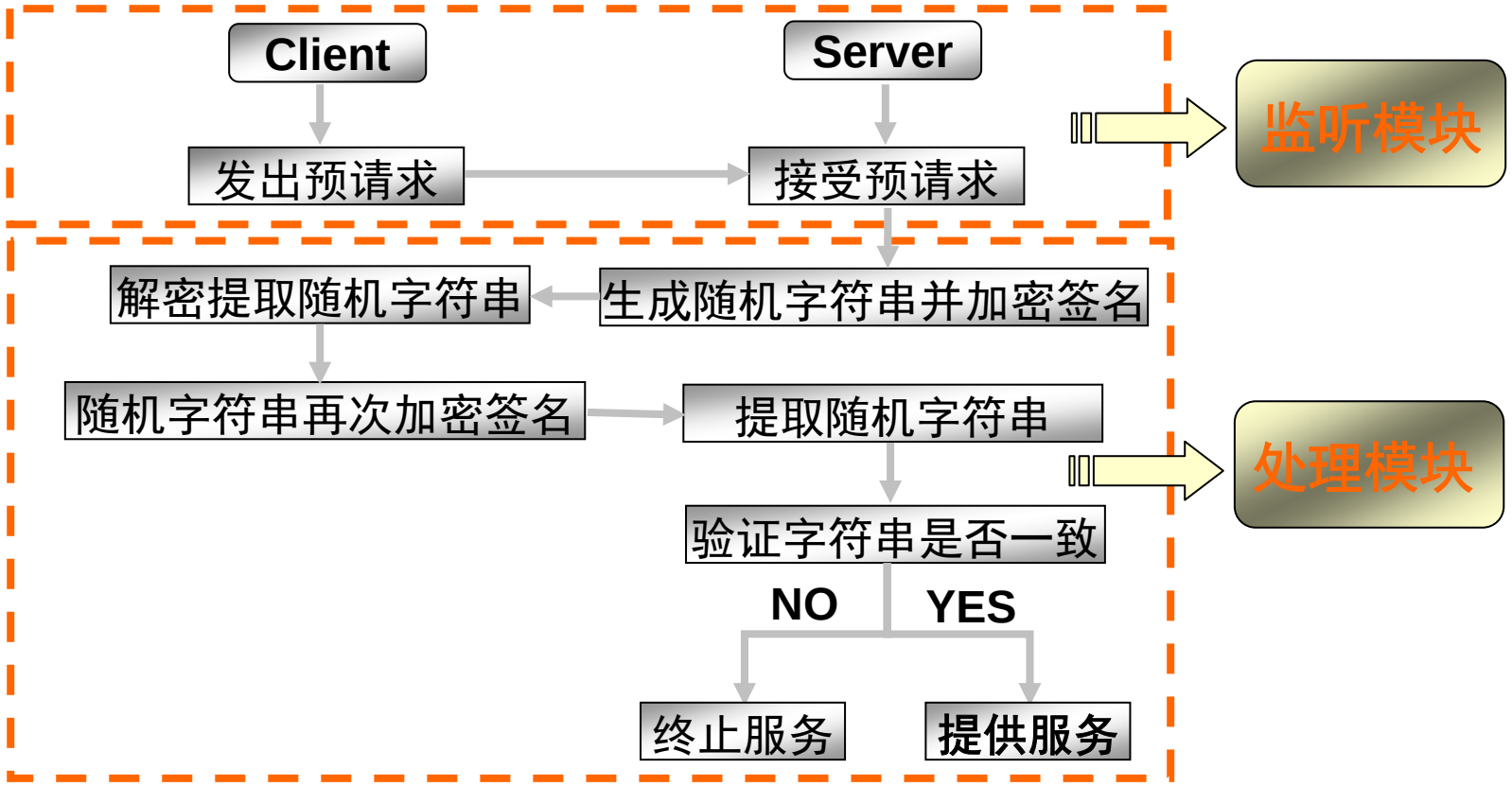
Secure Electronic Transactions (SET)协议

1. 应用于信用卡支付机制；
2. 由Visa 公司与MasterCard公司联合开发；
3. 使用双重验证，有效鉴别发送方与接收方；
4. 委托客户选定的金融机构管理数字证书；
5. 需要双方数字证书。

Set 协议与 SSL协议的比较

特性	SET	SSL
数据安全传输	Yes	Yes
验证客户身份	Yes	No
验证帐户的合法性	Yes	No
为商家验证支付方式	Yes	No
跟踪交易总额	Yes	No
验证商家的信用政策	Yes	No

基于数字证书的身份认证系统模型



电子商务支付网关

电子政务系统网络结构

远程访问和维护：

内网设计：

外网设计：

网间互连：

•进行层次化设计：核心层、汇聚层、接入层

•将外网的WEB系统和邮件系统等组成

防火墙（VPN隧道方式）保证通过

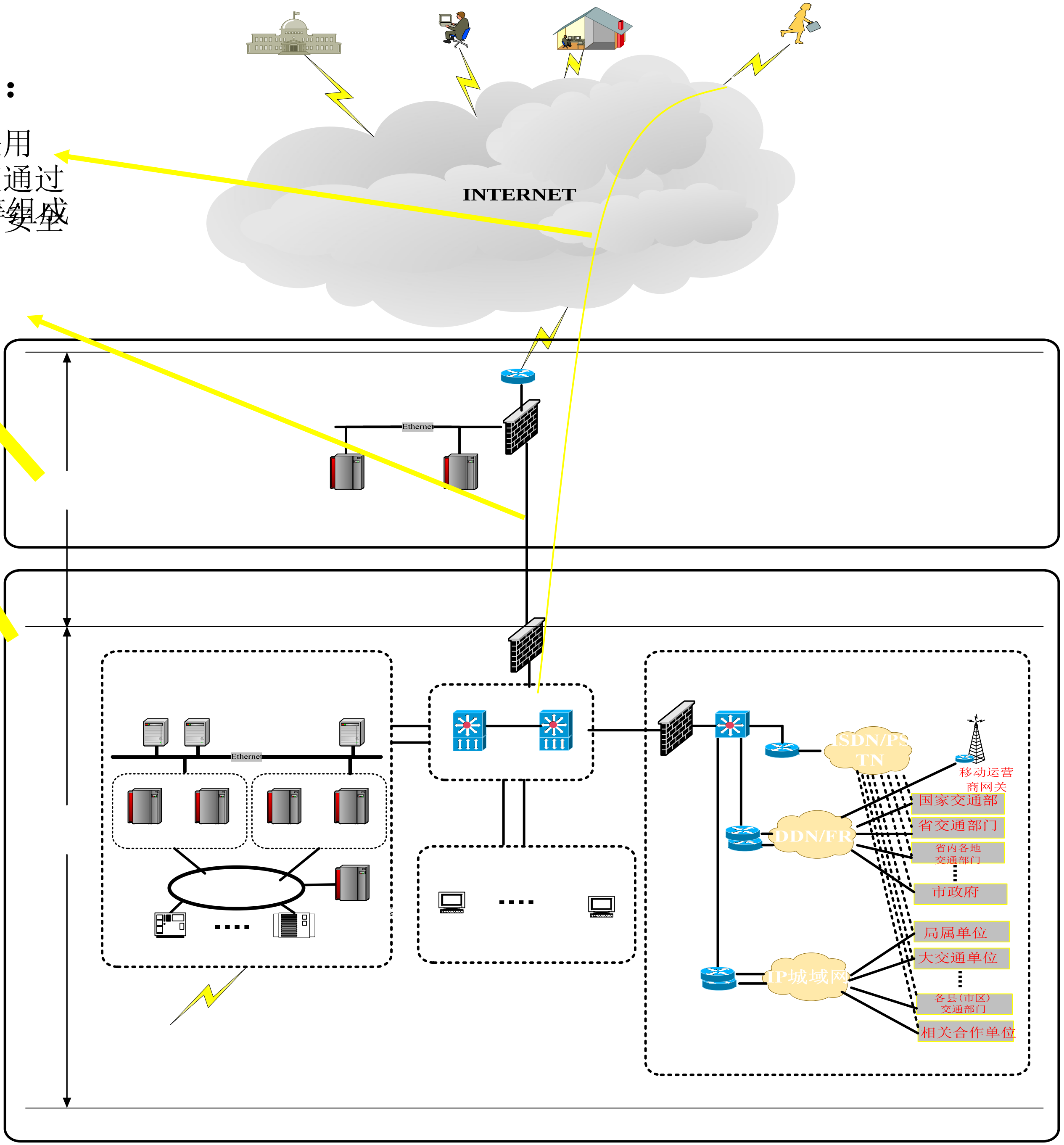
•安全性方面的问题和考虑

•核心交换机采用CISCO Catalyst4506双机集群

•可扩展性方面的考虑

•重要服务器做集群

•存储区域网做存储备份



（资料来源：戴伟辉，《浙江省宁波市交通信息网络平台设计》）

研讨题：拇指花运营系统安全分析

- 根据本课程讲述过的拇指花运营系统，思考以下问题：
- 上述系统中可能存在哪些安全问题？
- 你认为应采取什么样的措施来解决上述安全问题？
- 在以上措施中运用了哪些电子商务的安全技术？

拇指花彩信业务

“拇指花”是一种以鲜花束为视觉主体的全新的彩信产品，旨在使彩信成为特定的日常交际媒介，它给用户一种用手机送花的特别体验。

拇指花的创意

借用鲜花的符号价值

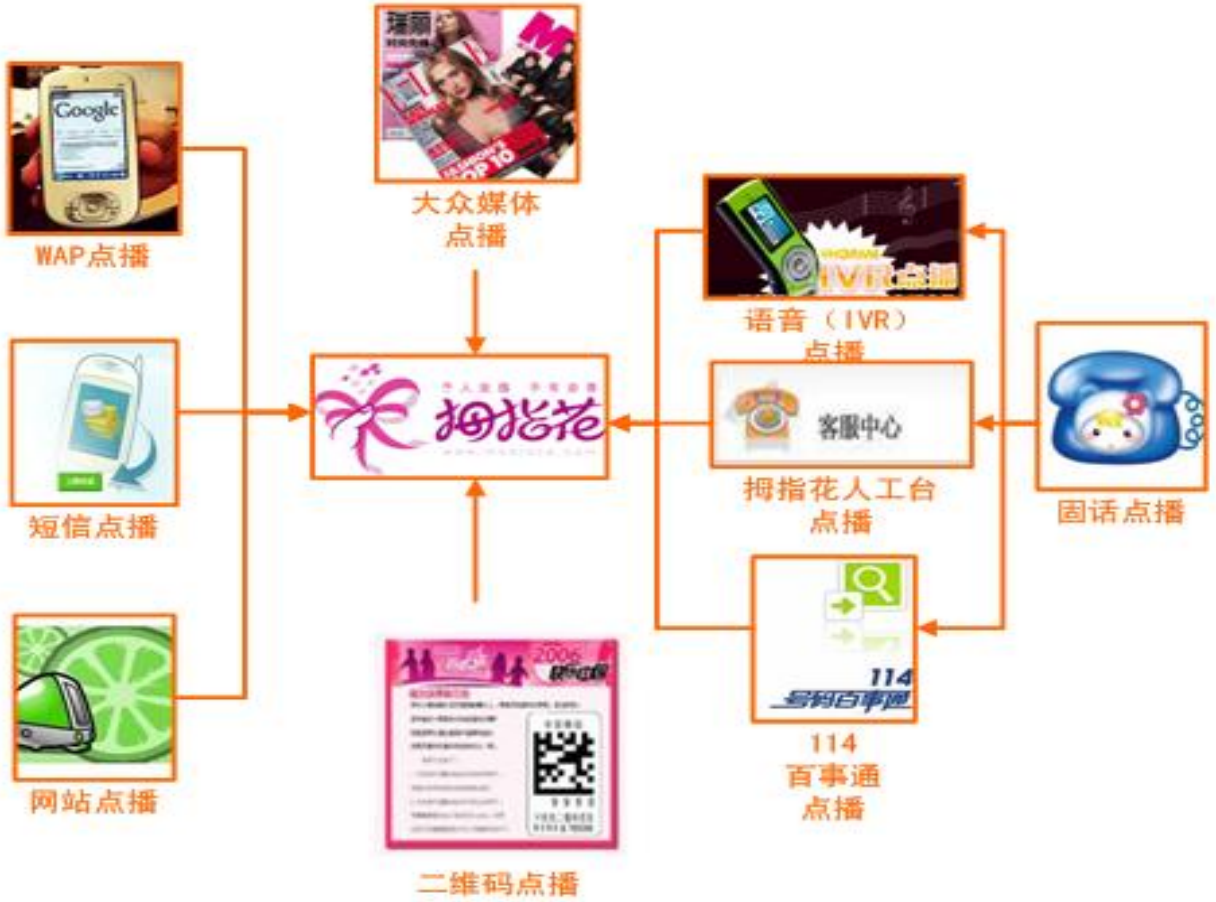
创造基于手机发送的情感礼物

形成手机问候的规则

将短信问候升级为彩信问候

挖掘“非接触时代”的快速情感消费市场

运营流程


WAP点播
大众媒体
点播
语音（IVR）
点播
短信点播
拇指花
客服中心
拇指花人工台
点播
固话点播
网站点播
114
百事通
点播
二维码点播