高级网络安全研究与应用——

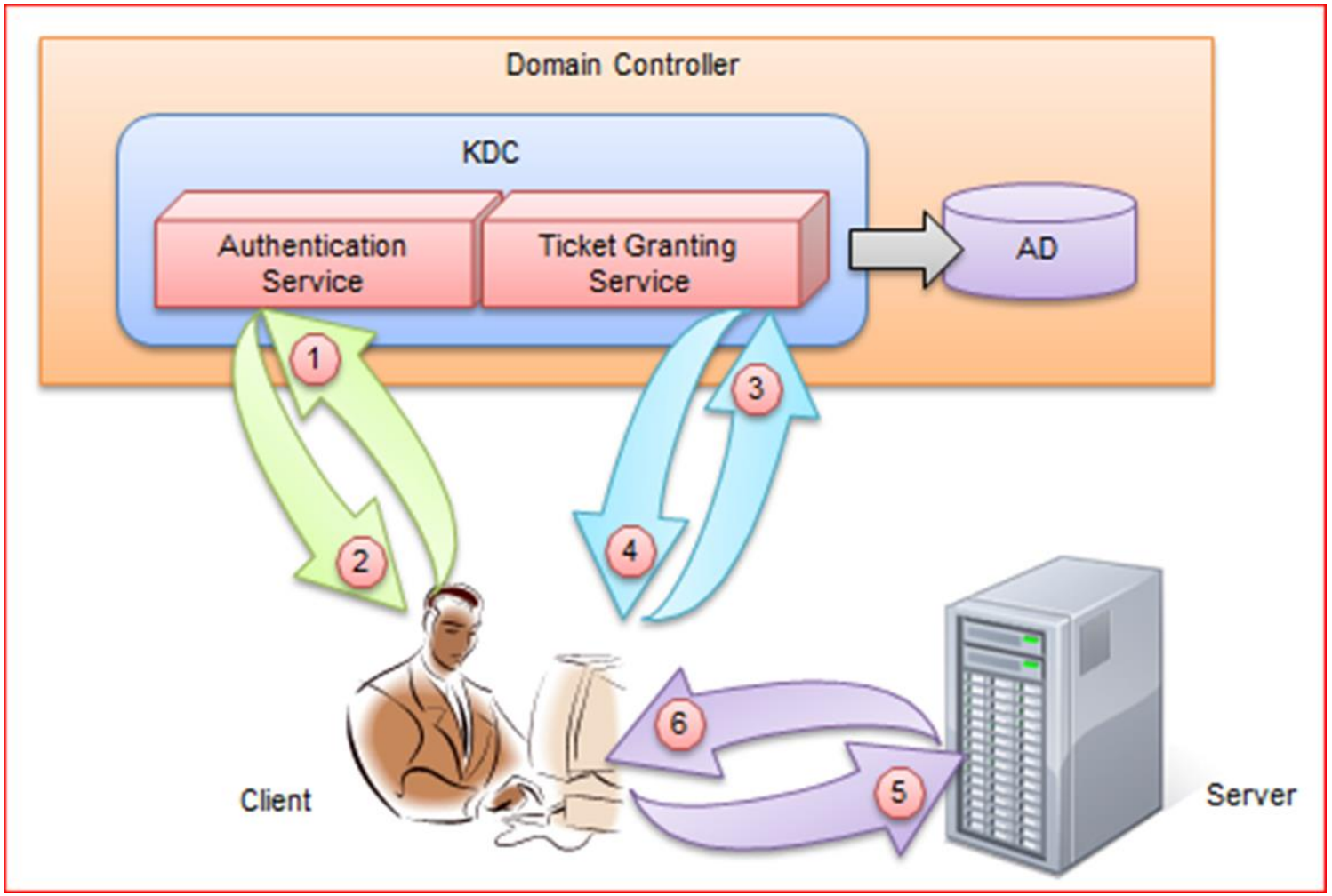
# 身份与认证

北京邮电大学

郑康锋 zkfbupt@163.com

伍淳华 wuchunhua@bupt.edu.cn

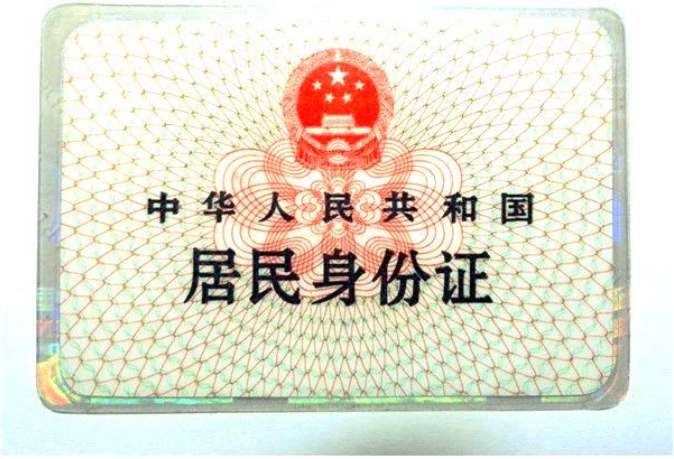
# 请猜


Domain Controller
KDC
Authentication Service
Ticket Granting Service
AD
1
2
3
4
5
6
Client
Server

# 身份与认证

- 身份
- 身份认证
- 身份安全

# 什么是身份？


中华人民共和国
居民身份证


香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD
中智能
SAN, Chi Nan
3947 2535 5174
出生日期 Date of Birth
01-01-1988 女F
***AZ
簽發日期 Date of Issue
(01-99)
15-09-18
C668668(E)


中华人民共和国
居民身份证
签发机关 上海市公安局徐汇分局
有效期限 2005.10.08-2025.10.08


香港永久性居民身份證
HONG KONG PERMANENT IDENTITY CARD
李智能
LEE, Chi Nan
樣本 SAMPLE
2621 2535 5174
出生日期 Date of Birth
01-01-1968 女 F
***AZ
簽發日期 Date of Issue
(01-79)
15-09-03
C668668(E)

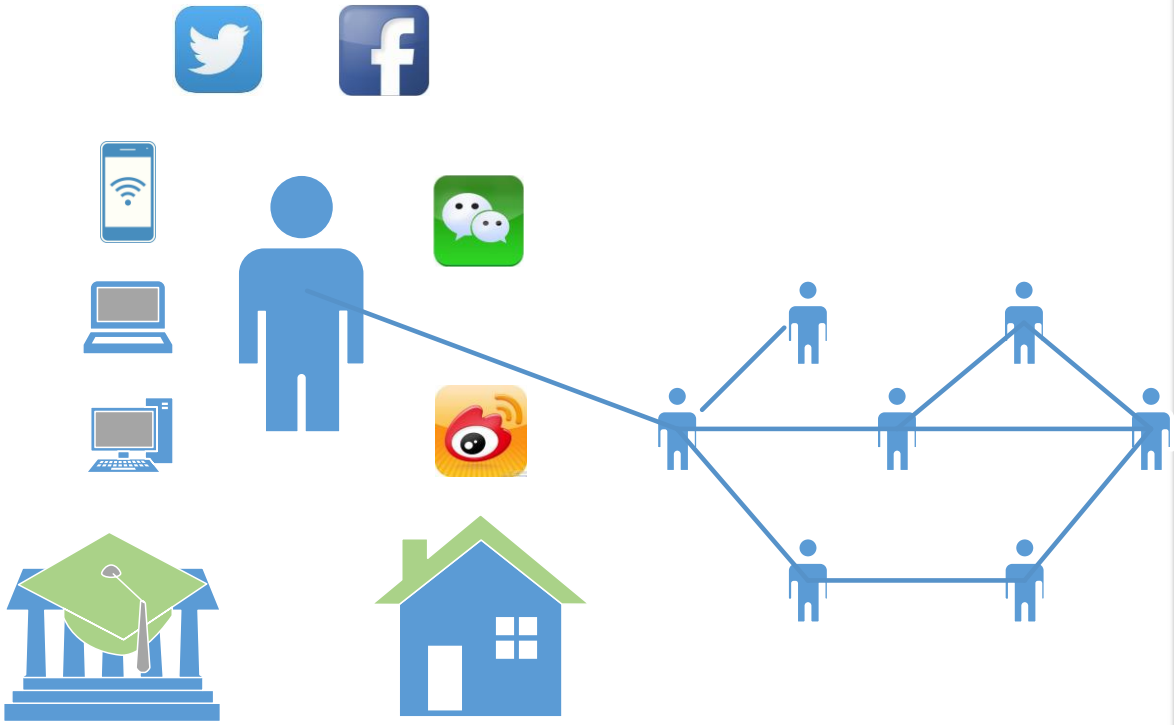
# 什么是身份？

**身分**，亦作“**身份**”。指出身和社会地位。见《宋书·王僧达传》：“固宜退省身分，识恩之厚，不知报答，当在何期。”

**身份认证**（Authentication）是证实用户的真实身份与其所声称的身份是否符合的过程，从而确定该用户是否具有对某种资源的访问和使用权限。

身份认证通过标识和鉴别用户的身份，提供一种判别和确认用户身份的机制。

# 什么是身份？



- 自有
  - 眼睛胳膊腿等
  - 声音、相貌等
  - 性格、人格等
- 社会
  - 家庭、朋友、单位
  - 网友、牌友、棋友
- 虚拟
  - 微信、微博、抖音
  - 游戏
- 持有
  - 手机、电脑
  - 学校、家

# 身份认证

- 认证依据
  - 基于信息秘密的身份认证
  - 基于信任物体的身份认证
  - 基于生物特征的身份认证
  - 步态、鼠标、键盘等等
  - MAC、IP、域名、手机号码、手机、姓名等
- 认证技术：生物特征识别、证书、签名等
- 鉴别机制： Kerberos、X.509、量子
- 认证体制：PKI、IBC

# 身份认证分类

- 基于信息秘密的身份认证

  根据你所知道的信息来证明你的身份(what you know ）；

- 基于信任物体的身份认证

  根据你所拥有的东西来证明你的身份(what you have ）；

- 基于生物特征的身份认证

  直接根据独一无二的身体特征来证明你的身份(who you are ）；

# 基于信息秘密的身份认证

所谓的秘密信息指用户所拥有的秘密知识，如：

- 用户ID
- 口令
- 密钥

身份认证方式：

- 基于帐号和口令的身份认证
- 基于对称密钥的身份认证
- 基于密钥分配中心的身份认证（Kerberos）
- 基于数字证书的身份认证（PKI）

# 基于信任物体的身份认证

- 根据你拥有的物体认证身份
  - 古代虎符、腰牌
  - 智能卡 信用卡
  - 验证码
  - 动态口令 U

# 基于生物特征的身份认证

- 生物特征认证指通过计算机利用人体固有的物理特征或行为特征鉴别个人身份。

- 美国中央情报局就曾一直使用语音识别系统对拉登的录音进行鉴识。拉登的音像信息每一次公布，美国情报部门都会通过语音鉴识技术来辨别其真伪，2010年，正是拉登的信使艾哈迈德在一次电话通信中被情报部门锁定，致使拉登的行踪暴露。目前的语音鉴识技术已经相当成熟，实际上，早在上世纪70年代，美国情报部门就开始使用这一技术监测前苏联领导人。

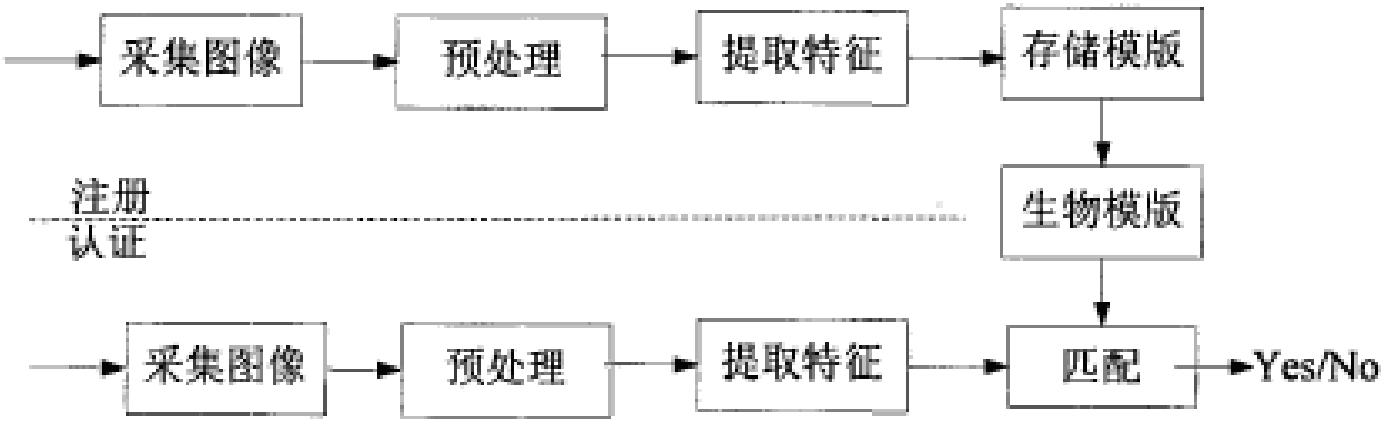
# 基于生物特征的身份认证

- 生物身体特征
  - 指纹
  - 脸部
  - 虹膜
- 生物行为特征
  - 签字
  - 步态
  - 语音
  - 鼠标和击键行为

# 基于生物特征的身份认证

作为身份认证的生物特征一般具备以下特性：

- 普遍性；即每一个人都应该具有这一特征。
- 唯一性；即每一个人在这一特征上有不同的表现。
- 稳定性；即这一特征不会随着年龄的增长和生活环境的改变而改变。
- 易采集；即这一特征应该便于采集和保存。
- 可接受；即人们是否能够接受这种生物识别方式。




生物特征识别过程

# 指纹

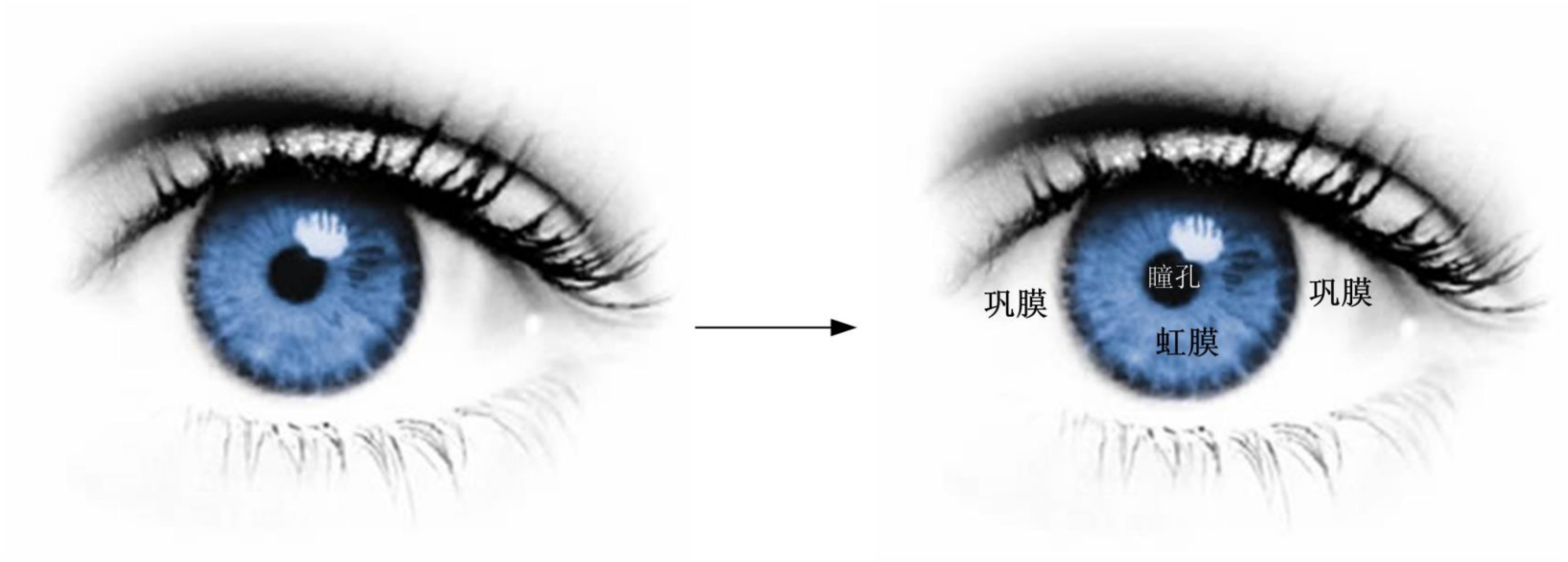

每个人包括指纹在内的皮肤纹路在图案、断点和交叉点上各不相同，呈现唯一性且终生不变。

- 总体特征是指那些用人眼直接就可以观察到的特征。包括纹形、模式区、核心点、三角点和纹数等。
- 局部特征是指指纹上节点的特征，这些具有某种特征的节点称为细节特征或特征点。断点、分叉点和转折点就称为"特征点"，其他还包括分歧点、孤立点、环点、短纹等。特征点的参数包括：方向、曲率、位置。

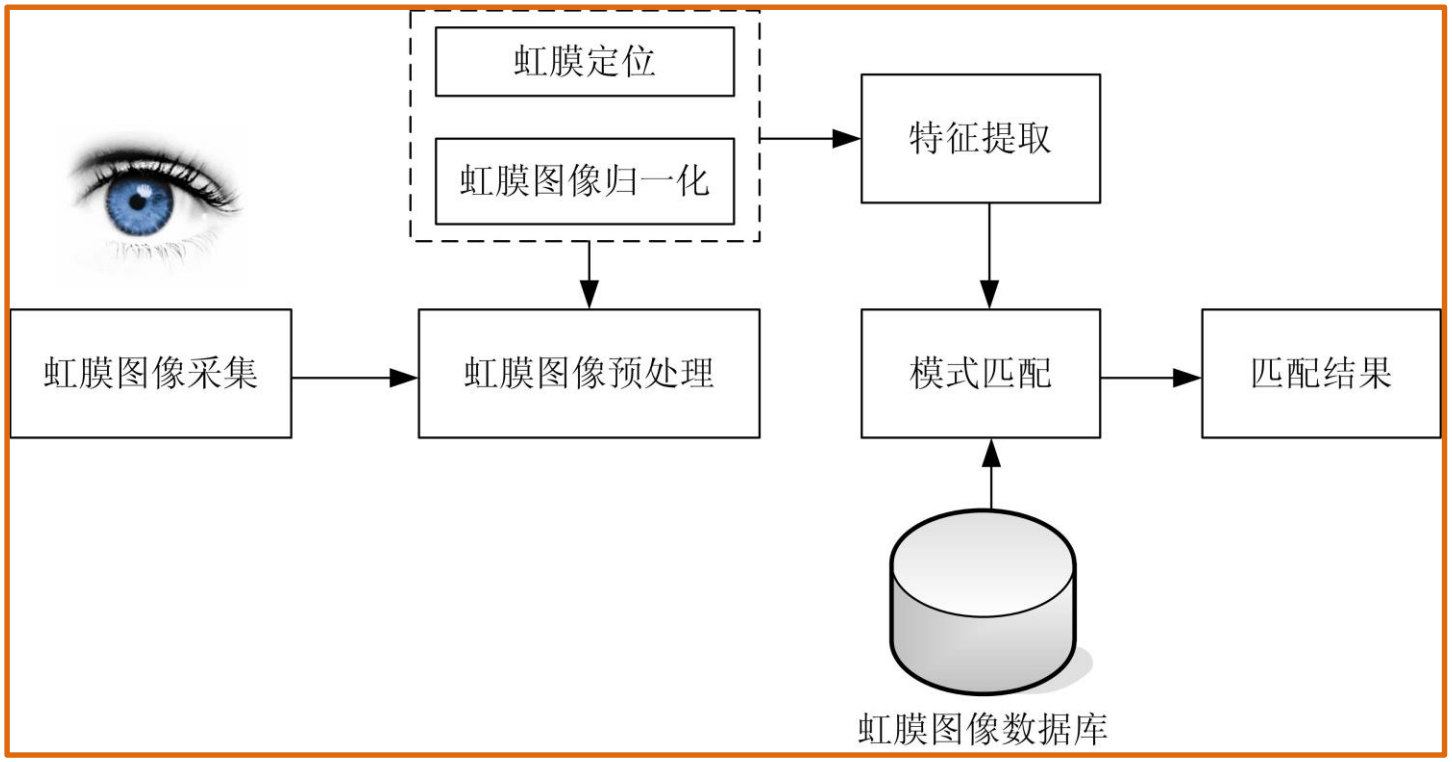
# 基于虹膜的身份认证

虹膜（眼睛中的彩色部分）是眼球中包围瞳孔的部分，上面布满极其复杂的锯齿网络状花纹，而每个人虹膜的花纹都是不同的。

虹膜识别技术就是应用计算机对虹膜花纹特征进行量化数据分析，用以确认被识别者的真实身份。



# 基于虹膜的身份认证




**实现虹膜认证需要以下步骤：**

虹膜图像采集->虹膜图像预处理->虹膜纹理的特征提取->模式匹配

身份与认证——

# 身份认证

# 基于Kerberos的认证方式

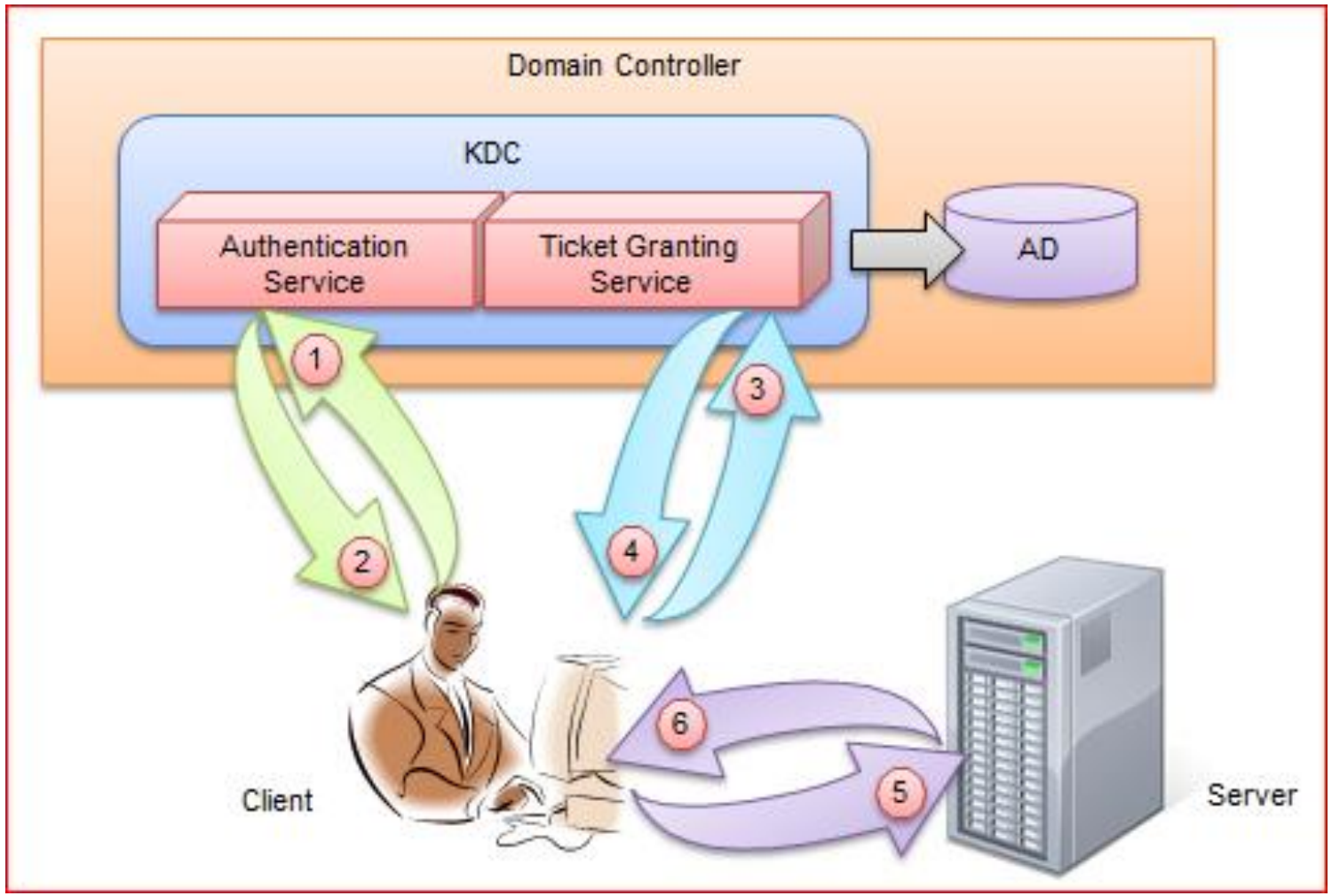
- Kerberos这一名词来源于希腊神话“三个头的狗”——地狱之门守护者

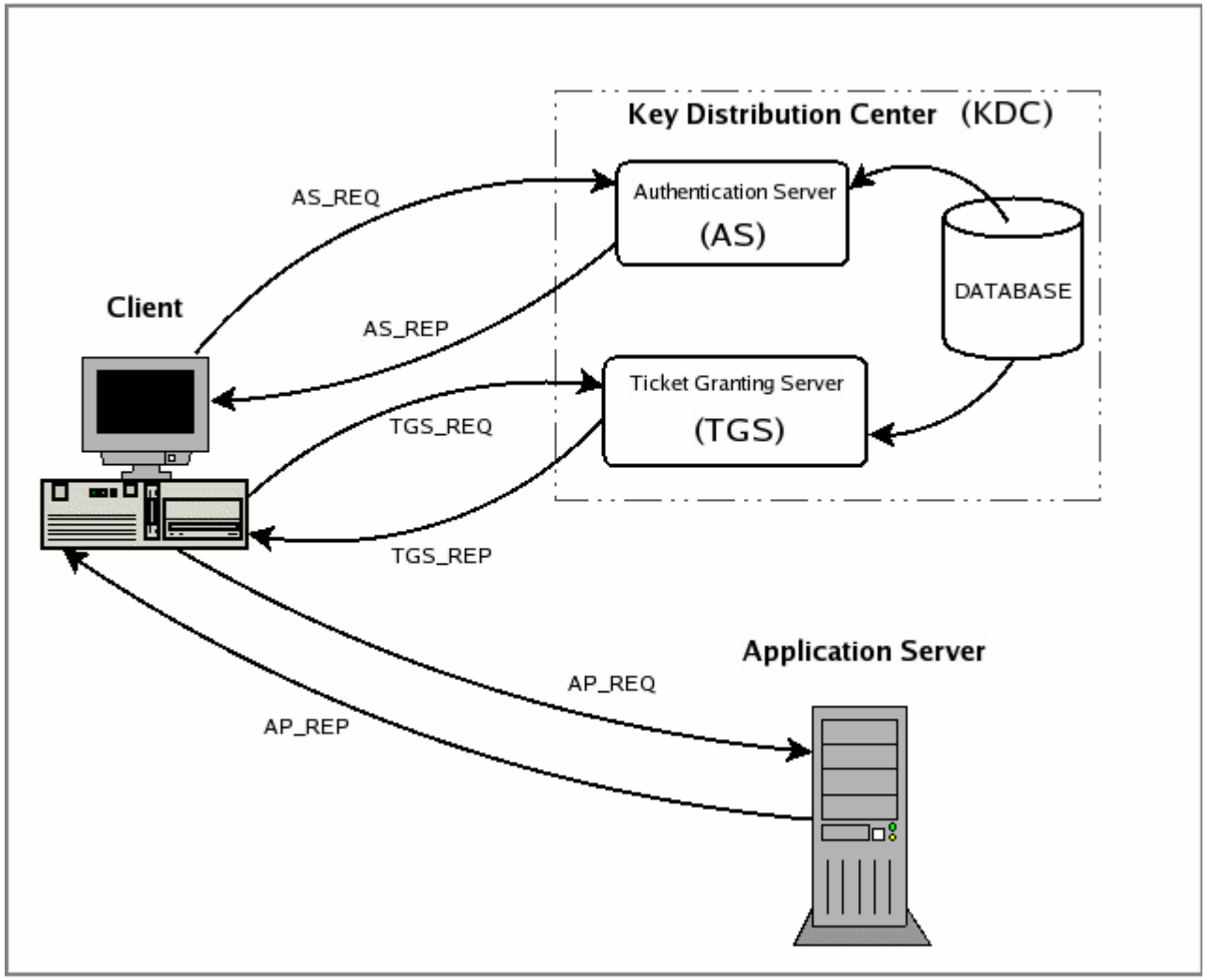

- Kerberos是一种用于身份认证业务的秘密密钥网络认证协议，最早由麻省理工学院(MIT)设计并开发，它的设计思想影响了以后的很多的身份认证业务。Kerberos使用数据加密标准DES加密算法来进行加密和认证，现在已发展到v5版本，实现工具Heimdal由瑞典皇家理工发布。

# 基于Kerberos的认证方式

- Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。

- 多用于组织内部，如局域网。


Domain Controller
KDC
Authentication Service
Ticket Granting Service
AD
1
2
3
4
5
6
Client
Server


Key Distribution Center (KDC)
Authentication Server
(AS)
DATABASE
Ticket Granting Server
(TGS)
Client
AS_REQ
AS_REP
TGS_REQ
TGS_REP
Application Server
AP_REQ
AP_REP

# 基于Kerberos的认证方式

- Kerberos主要涉及：

| | |
|---|---|
| Client | 请求服务的客户端 |
| Server | 提供服务的服务端 |
| KDC （Kerberos Distribution Center） | 提供认证的可信第三方 |

Kerberos起源于希腊神话，是一支守护着冥界长着3个头颅的神犬，在keberos Authentication中，Kerberos的3个头颅代表中认证过程中涉及的3方：Client、Server和KDC

# 基于Kerberos的认证方式

背景知识

- Long-term Key/Master Key：

在Security的领域中，在长期内保持不变的Key、以及由此派生的Key被称为Long-term Key。对于Long-term Key的使用有这样的原则：被Long-term Key加密的数据不应该在网络上传输。原因很简单，一旦这些被Long-term Key加密的数据包被恶意的网络监听者截获，在原则上，只要有充足的时间，他是可以通过计算获得你用于加密的Long-term Key。

- Short-term Key/Session Key：

由于被Long-term Key加密的数据包不能用于网络传送，所以我们使用另一种Short-term Key来加密需要进行网络传输的数据。由于这种Key只在一段时间内有效，即使被加密的数据包被黑客截获，等他把Key计算出来的时候，这个Key早就已经过期了。

# 基于Kerberos的认证方式

关键前提

对于一个Domain而言，KDC维护着一个存储着该Domain中所有帐户的Account Database（一般地，这个Account Database由AD来维护），也就是说，他知道属于每个Account的名称和派生于该Account Password的Master Key。

- KDC拥有Client的Master Key;
- KDC拥有Server的Master Key;

**Kerberos的基本原理是：在网络上建立一个集中保存用户名和密码的认证中心KDC（包含AS和TGS），进行用户的身份验证和授权。**

# 基于Kerberos的认证方式

Kerberos基本流程

1. Client向KDC申请TGT（Ticket Granting Ticket）。
2. Client通过获得TGT向KDC申请用于访问Server的Ticket。
3. Client最终向为了Server对自己的认证向其提交Ticket。

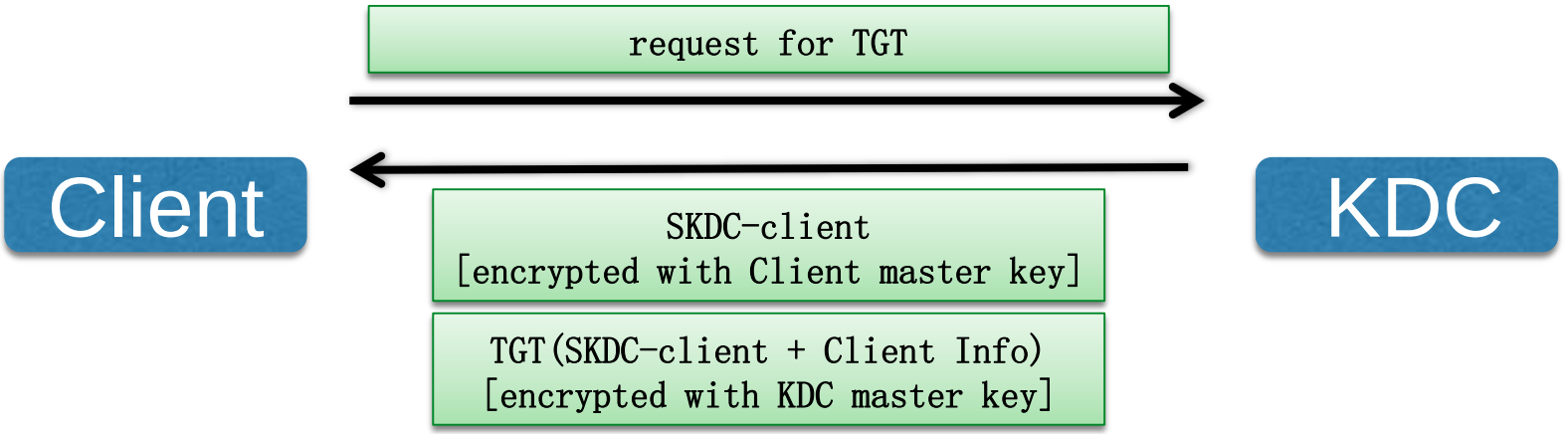
# 基于Kerberos的认证方式

## 1. Client向KDC申请TGT

① Client向KDC请求TGT；

② KDC生成一个$S_{KDC-client}$并用Client的MasterKey加密；
生成TGT($S_{KDC-client}$ + Client Info)并用KDC的MasterKey加密；
将这两个加密后的数据发送给Client；

③ Client收到后，用自己的MasterKey解密得到与KDC的Session Key-----$S_{KDC-client}$，并将该$S_{KDC-client}$和TGT缓存；

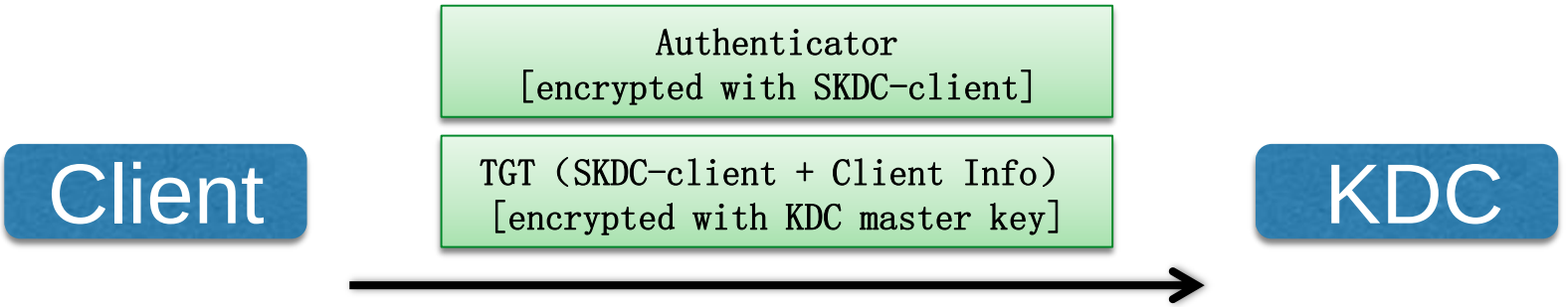


# 基于Kerberos的认证方式

2. Client通过TGT向KDC申请用于访问Server的Ticket

① Client用$S_{KDC-client}$加密自己的Authenticator(Client Info以及访问的Server)，连同TGT一并发给KDC;

② KDC用自己的MasterKey解密TGT得到$S_{KDC-client}$和Client Info;
再用$S_{KDC-client}$解密Authenticator得到Client Info，对两者进行比较;



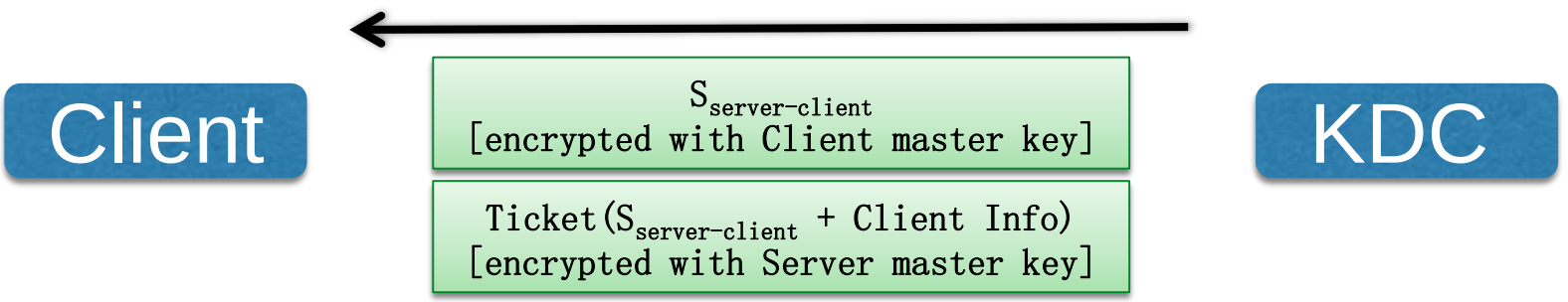
# 基于Kerberos的认证方式

2. Client通过TGT向KDC申请用于访问Server的Ticket

③ 验证成功，KDC生成$S_{server-client}$并用Client Master Key加密；

④ KDC生成Ticket($S_{server-client}$ + Client Info)并用Server Master Key加密；

⑤ KDC将两个加密后的数据发送给Client；

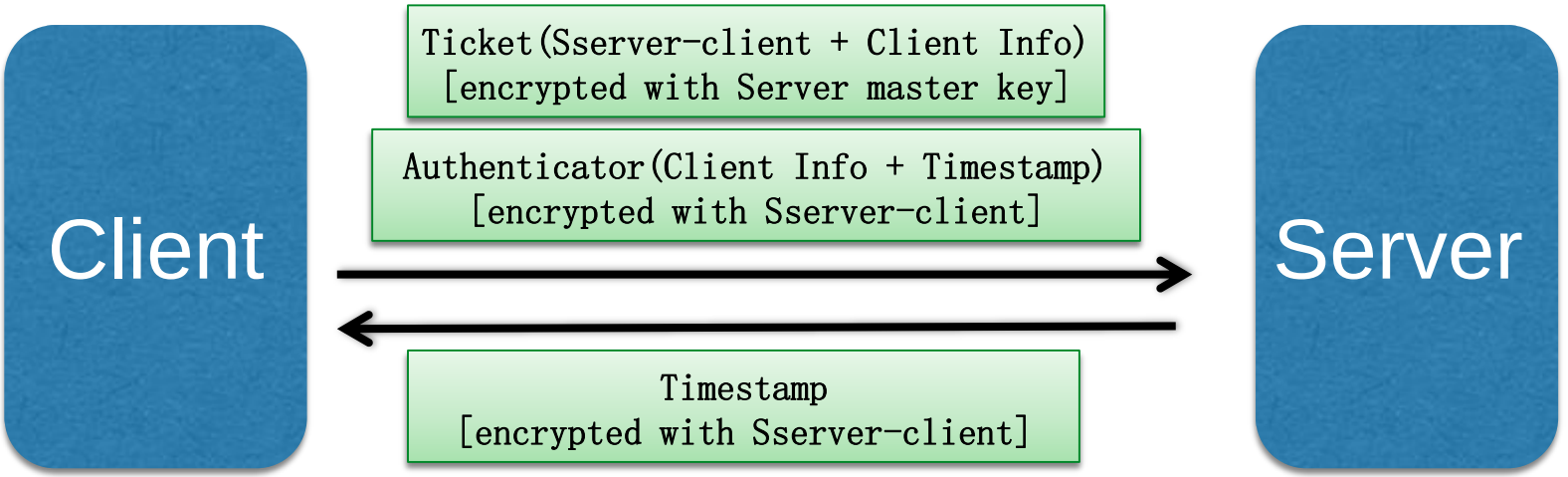


# 基于Kerberos的认证方式

3. Client为了Server对自己的认证向其提交Ticket

① Client用$S_{server-client}$加密自己的Authenticator(Client Info + Timestamp)，连同Ticket一并发给Server；

② Servers收到后用自己的MasterKey解密Ticket，得到$S_{server-client}$和Client Info；再用$S_{server-client}$ 解密Authenticator，得到Client Info和Timestamp，通过比较两者的Info实现对Client的认证；



# 基于Kerberos的认证方式

## 双向认证（Mutual Authentication）

- Kerberos一个重要的优势在于它能够提供双向认证
- 如果Client需要对他访问的Server进行认证，会在它向Server发送的Credential中设置一个是否需要认证的Flag。Server在对Client认证成功之后，会把Authenticator中的Timestamp提取出来，通过Session Key进行加密，当Client接收到并使用Session Key进行解密之后，如果确认Timestamp和原来的完全一致，那么他可以认定Server正式他试图访问的Server。

# 基于Kerberos的认证方式

Kerberos优势

- 高效率的身份认证
- Server和KDC不需要维护SessionKey列表
- 双向认证
- 无需保证主机、网络的安全性

# 基于Kerberos的认证方式

## Kerberos缺陷

- Kerberos身份认证采用的是对称加密机制，加密和解密使用的是相同的密钥，交换密钥时的安全性比较难以保障。
- Kerberos要求参与通信的主机的时钟同步。票据具有一定有效期，因此，如果主机的时钟与Kerberos服务器的时钟不同步，认证会失败。默认设置要求时钟的时间相差不超过10分钟。
- 对KDC安全性的高度依赖。所有用户使用的密钥都存储于中心服务器中，危及服务器的安全的行为将危及所有用户的密钥。

# 基于PKI的认证方式

公钥基础设施PKI（Public Key Infrastructure），是一种运用非对称密码技术来实施并提供安全服务的具有普适性的网络安全基础设施。

- 目前网络安全建设的基础与核心
- 电子商务安全实施的基本保障

# 基于PKI的认证方式

背景：

随着网络技术和信息技术的发展，电子商务已逐步被人们所接受，并在得到不断普及。但由于各种原因，国内电子商务的安全性仍不能得到有效的保障。

- 常规业务---利用商场开具的发票和客户现场支付商品费用，无须担心发生纠纷和无凭证可依。
- 电子商务---不是现场交易，如何确认双方合法身份、保证交易信息安全保密？

# 基于PKI的认证方式

电子交易的安全问题：

- **保密性**：如何保证电子商务中涉及的大量保密信息在公开网络的传输过程中不被窃取；
- **完整性** ：如何保证电子商务中所传输的交易信息不被中途篡改及通过重复发送进行虚假交易；
- **身份认证与授权** ：在电子商务的交易过程中，如何对双方进行认证，以保证交易双方身份的正确性；
- **不可否认性** ：在电子商务的交易完成后，如何保证交易的任何一方无法否认已发生的交易。

# 基于PKI的认证方式

PKI的工作内容：

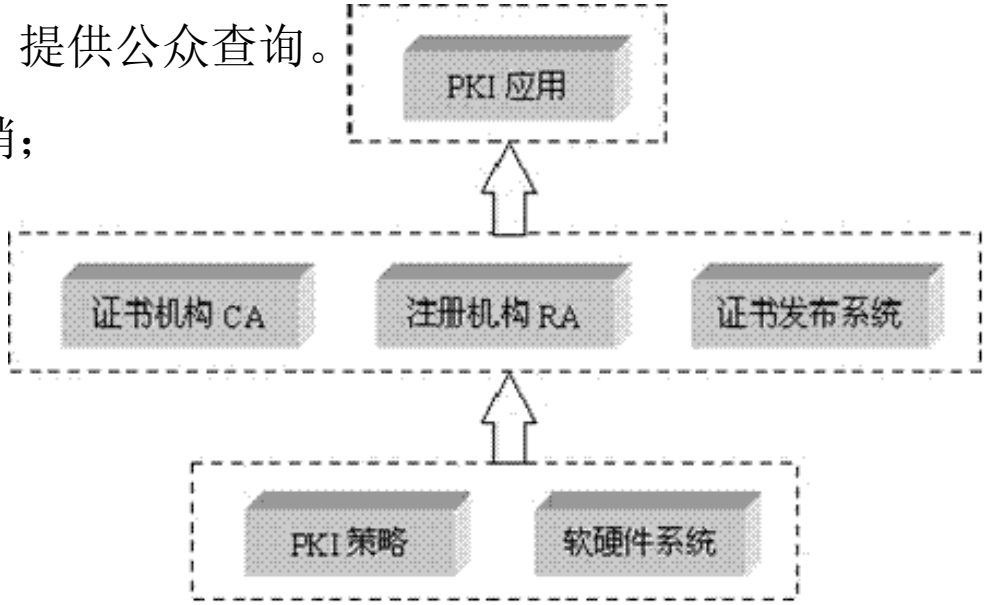
- PKI采用证书进行公钥管理，通过第三方的可信任机构（认证中心，即CA），把用户的公钥和用户的其他标识信息捆绑在一起，其中包括用户名和电子邮件地址等信息，以在Internet网上验证用户的身份。

- PKI把公钥密码和对称密码结合起来，在Internet网上实现密钥的自动管理，保证网上数据的安全传输。

# 基于PKI的认证方式

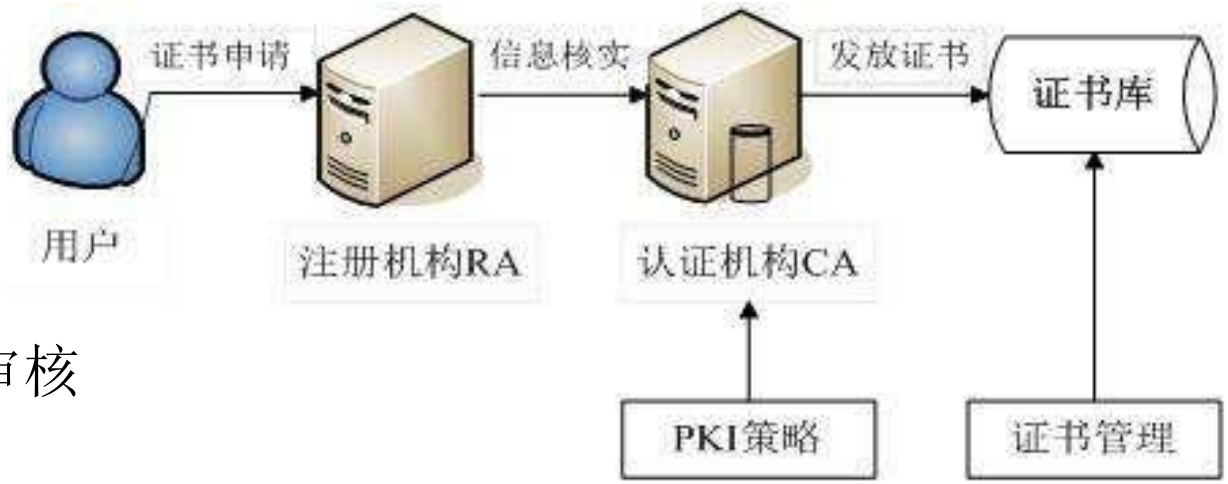
PKI组成：

- **CA(认证中心)**：证书的签发机构，PKI的核心，是PKI应用中权威的、可信任的、公正的第三方机构。它对任何一个主体的公钥进行公证，通过签发证书将主体与公钥进行捆绑，负责确认身份和创建数字证书以建立一个身份和一对公/私密钥间的联系。
- **RA(注册中心)**：负责接收用户的用户注册和申请鉴别，审核用户的身份，并决定是否同意CA给申请者签发数字证书。
- **证书发布库**：证书的集中存放地，提供公众查询。
- **策略**：密钥备份与恢复、证书撤销；
- **应用接口**：API等；



# 基于PKI的认证方式

PKI证书申请：




- 用户申请
- 注册机构(RA)审核
- CA发行证书
- 注册机构证书转发
- 用户证书获取

# 基于PKI的认证方式

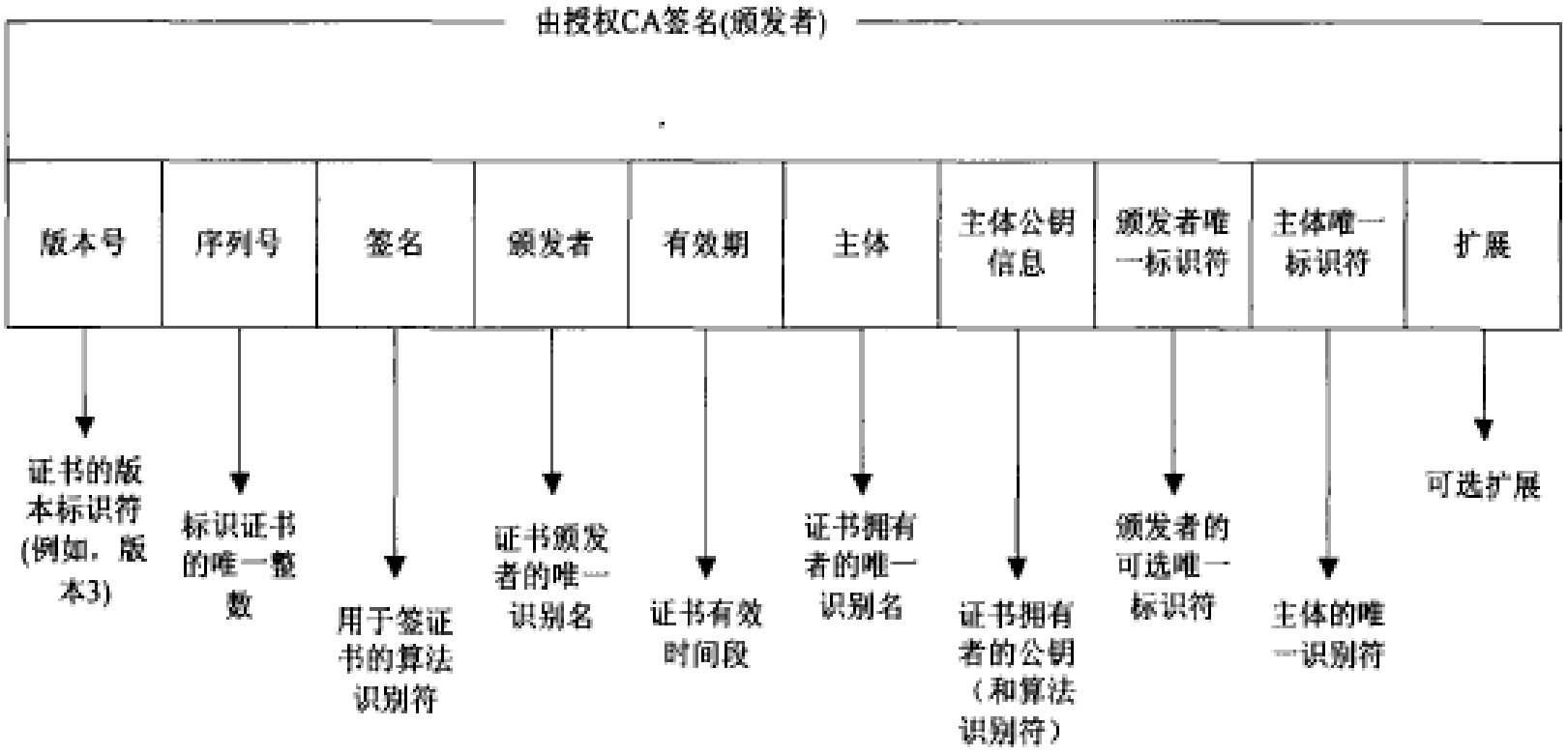
数字证书包含：

- 用户身份信息；
- 用户公钥信息，保证数字信息传输的完整性；
- 身份验证机构的数字签名，确保证书信息的真实性；
- 数字签名，保证数字信息的不可否认性；

# 基于PKI的认证方式

由国际电联电信委员会（ITU-T）制定的X.509数字证书标准被广泛使用。

目前使用最多的是X.509v3标准：



# 基于PKI的认证方式

使用证书对数据验证的过程：

- 将客户端发来的数据解密（如解开数字信封）
- 将解密后的数据分解成原始数据，签名数据和客户证书三部分
- 用CA根证书验证客户证书的签名完整性
- 检查客户证书是否有效（当前时间在证书结构中的所定义的有效期内）
- 客户证书验证原始数据的签名完整性

# 基于PKI的认证方式

PKI的优势：

- 采用公开密钥密码技术，能够支持可公开验证并无法仿冒的数字签名；
- 密码技术的采用使PKI具有机密性；
- 由于数字证书可以由用户独立验证，不需要在线查询，原理上能够保证服务范围的无限制地扩张，这使得PKI能够成为一种服务巨大用户群的基础设施；
- PKI具有极强的互联能力；
- PKI提供了证书的撤销机制，提供了纠错途径；

身份与认证——

# 身份安全

# 身份安全

**身份相关众多，但哪个真正/绝对属于你?**

人

- 指纹/虹膜/面部
- 声音/图像/视频
- 字迹/足迹
- 步态/习惯动作
- 性格/人格/情绪
- 同学/亲戚/朋友

- 手机/电脑/平板
- 微信/微博/抖音
- 身份证/银行卡
- 学校/家/单位
- 汽车/自行车

- MAC/IP
- ID/昵称
- GIS
- 好友/赞
- 网络行为
- 帖子推文

# 身份安全

## 身份在网络空间的情况

关联关系

# 身份面临的安全问题

- 欺骗：ARP欺骗、IP欺骗、DNS欺骗等
- 诈骗：假冒家人、同学、机关工作人员
- 假冒：冒用身份（上学、工作等等）
- 中间人：伪基站、伪AP等
- DoS：认证协议DoS、重放攻击、注册信息DoS
- 各类攻击：隧道、黑洞、女巫等攻击

# 身份面临的安全问题

## 身份安全

- 身份伪造
- 身份嫁接
- 身份采购

## 身份认证过程安全

- 阻断
- 篡改
- 伪造

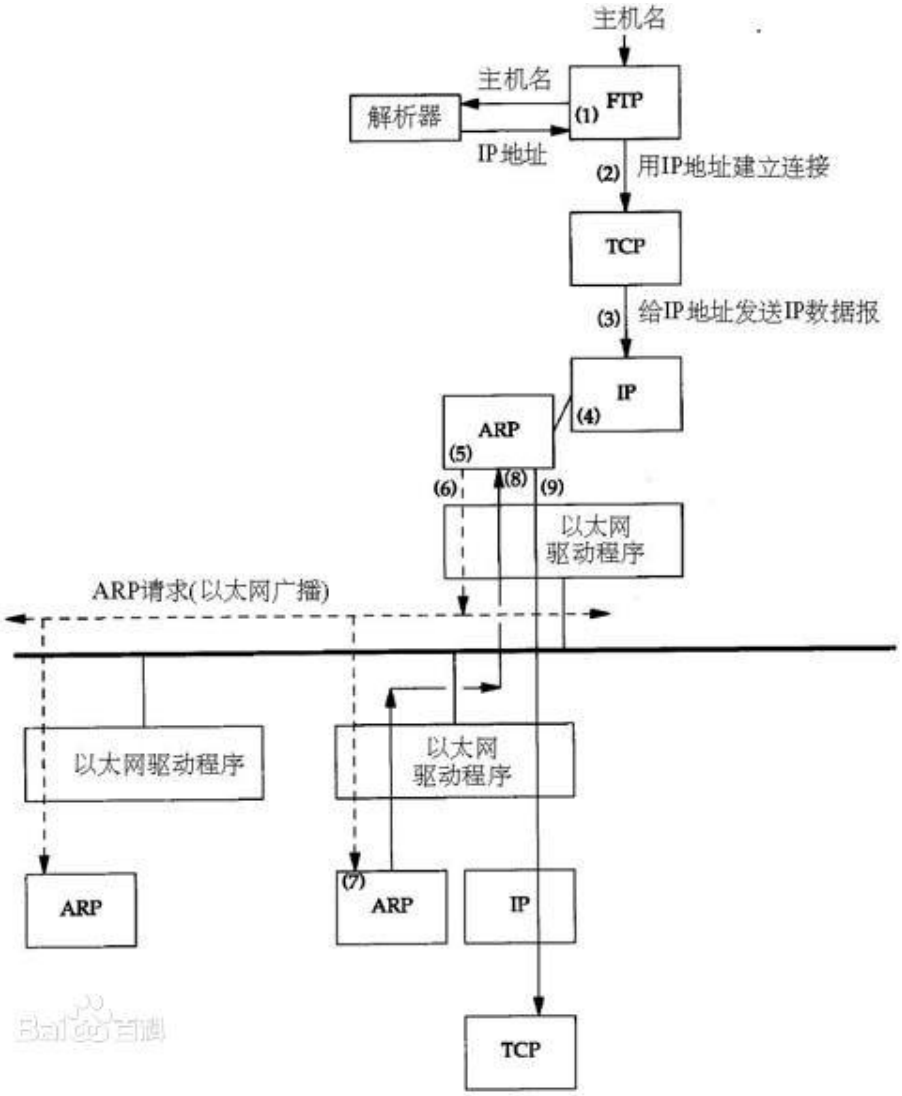
**身份安全示例——**

# 间接类

## ARP欺骗/DNS欺骗/中间人攻击

# ARP协议

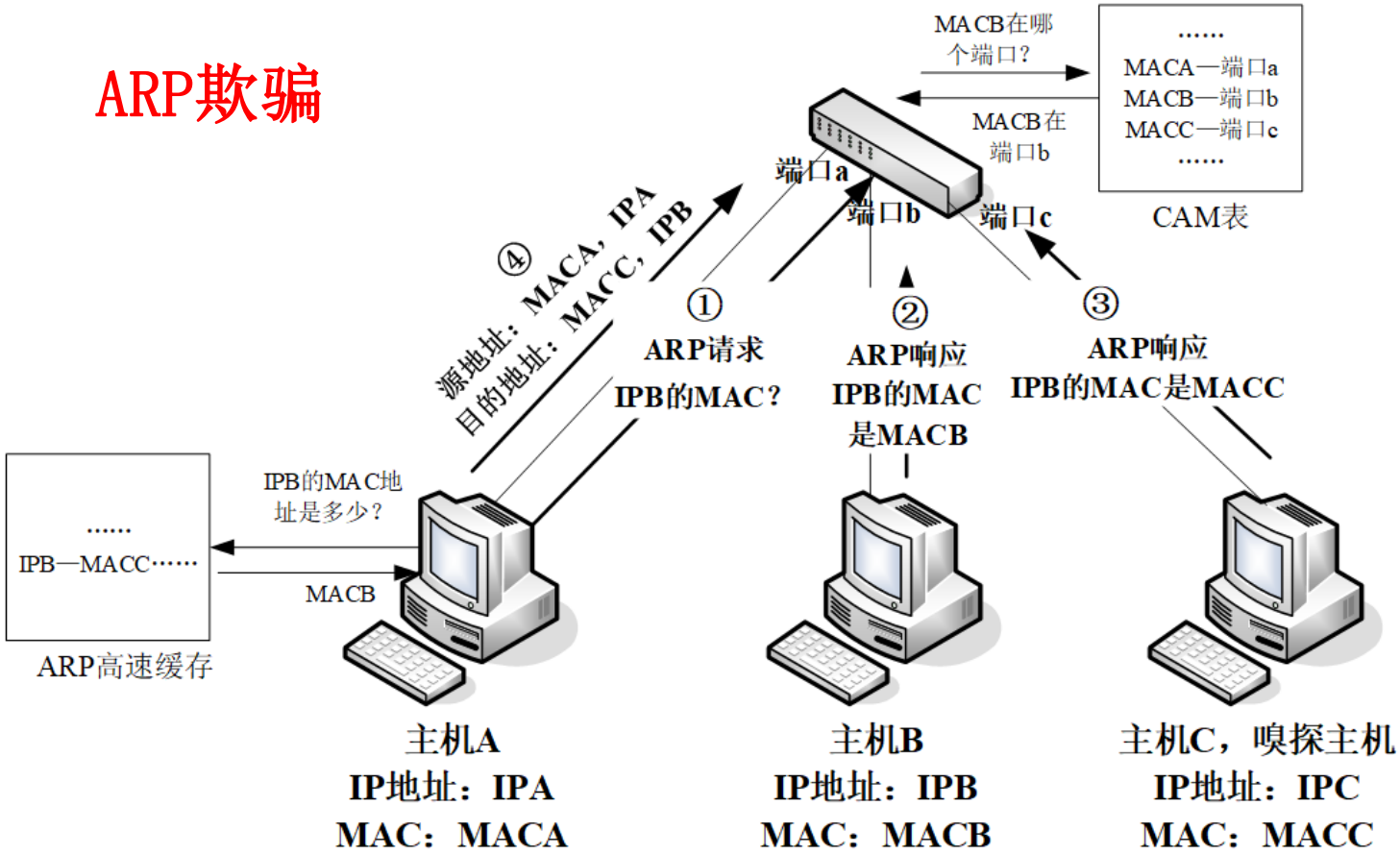
- 地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。



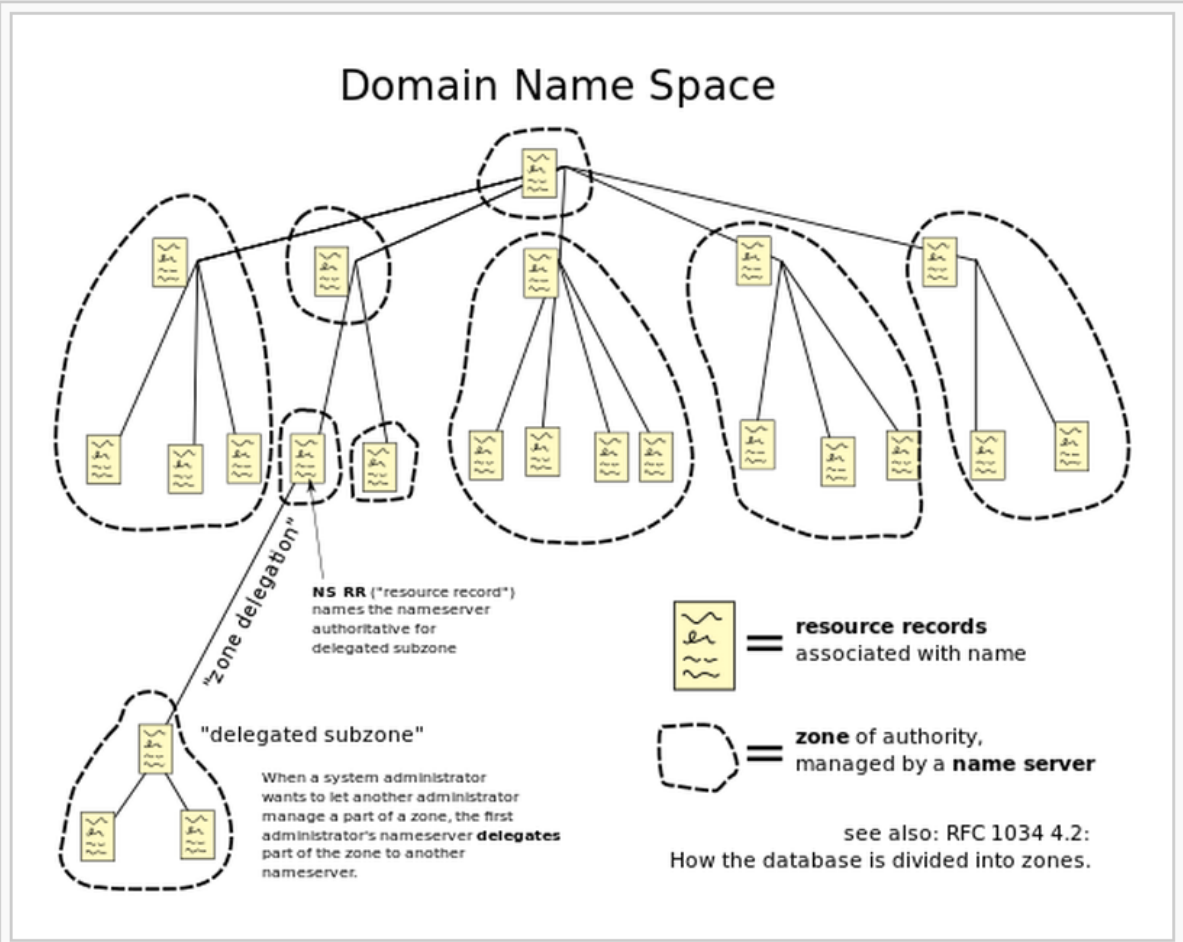

注：资料及图片来自于百度百科。

# ARP攻击技术

- ARP欺骗

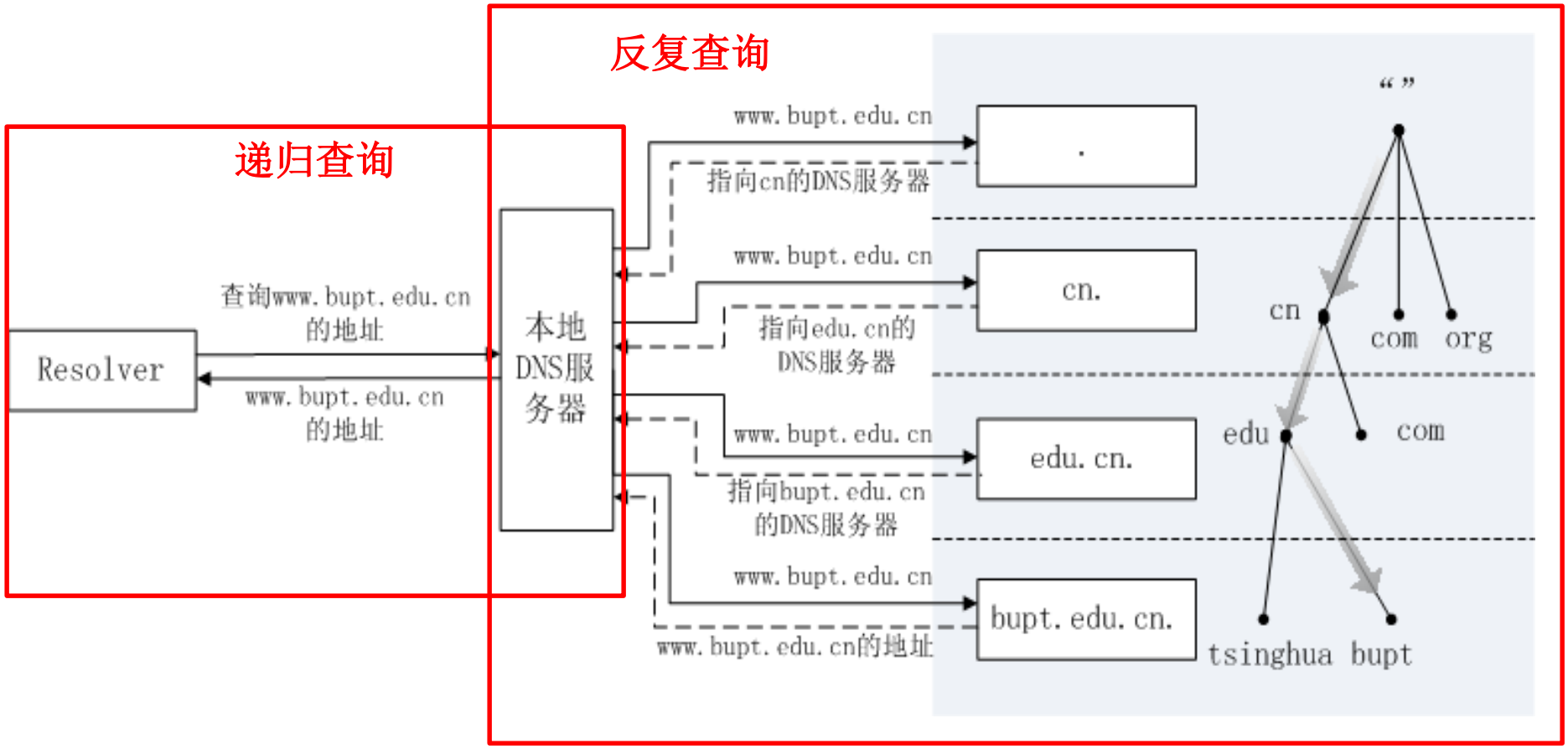


# Domain Name Space




The hierarchical Domain Name System, organized into zones, each served by a name server

# DNS工作流程

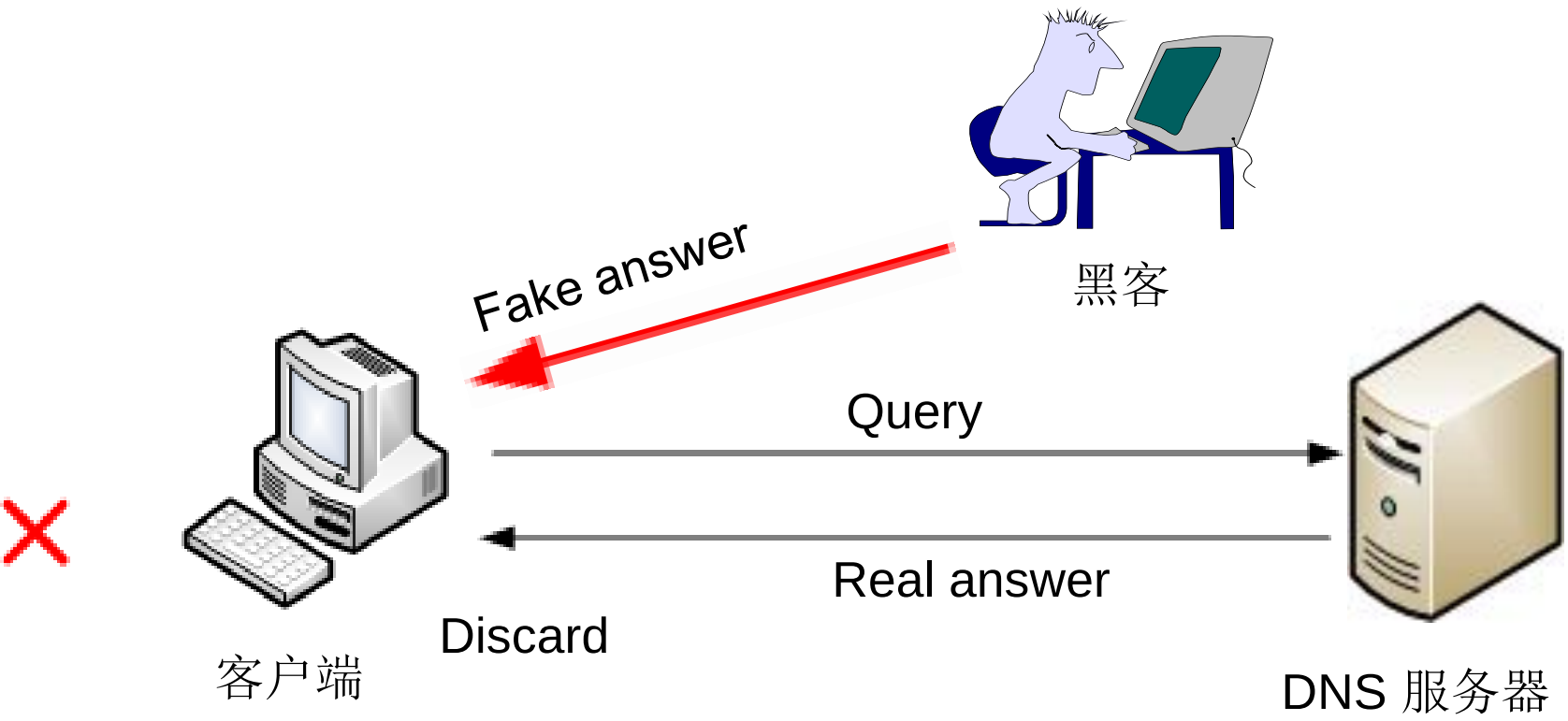

反复查询
递归查询
查询www.bupt.edu.cn
的地址
Resolver
www.bupt.edu.cn
的地址
本地
DNS服
务器
www.bupt.edu.cn
指向cn的DNS服务器
www.bupt.edu.cn
指向edu.cn的
DNS服务器
www.bupt.edu.cn
指向bupt.edu.cn
的DNS服务器
www.bupt.edu.cn
www.bupt.edu.cn的地址
.
cn.
edu.cn.
bupt.edu.cn.
“ ”
cn
com
org
edu
com
tsinghua
bupt

# DNS安全威胁

- DNS应答包被客户端接受需要满足以下五个条件
  - 1、应答包question域和请求包question域的域名信息一致。
  - 2、应答包的Transaction ID和请求包中的Transaction ID一致。
  - 3、应答包的源IP地址与请求包的目的IP地址一致。
  - 4、应答包的目的IP地址和端口与请求包的源IP地址和端口一致。
  - 5、第一个到达的符合以上四个条件的应答包。
- 从以上五个条件可以看出，最初设计DNS时没有考虑它的安全问题，这导致DNS协议存在很多漏洞，这使得DNS很容易受到攻击。

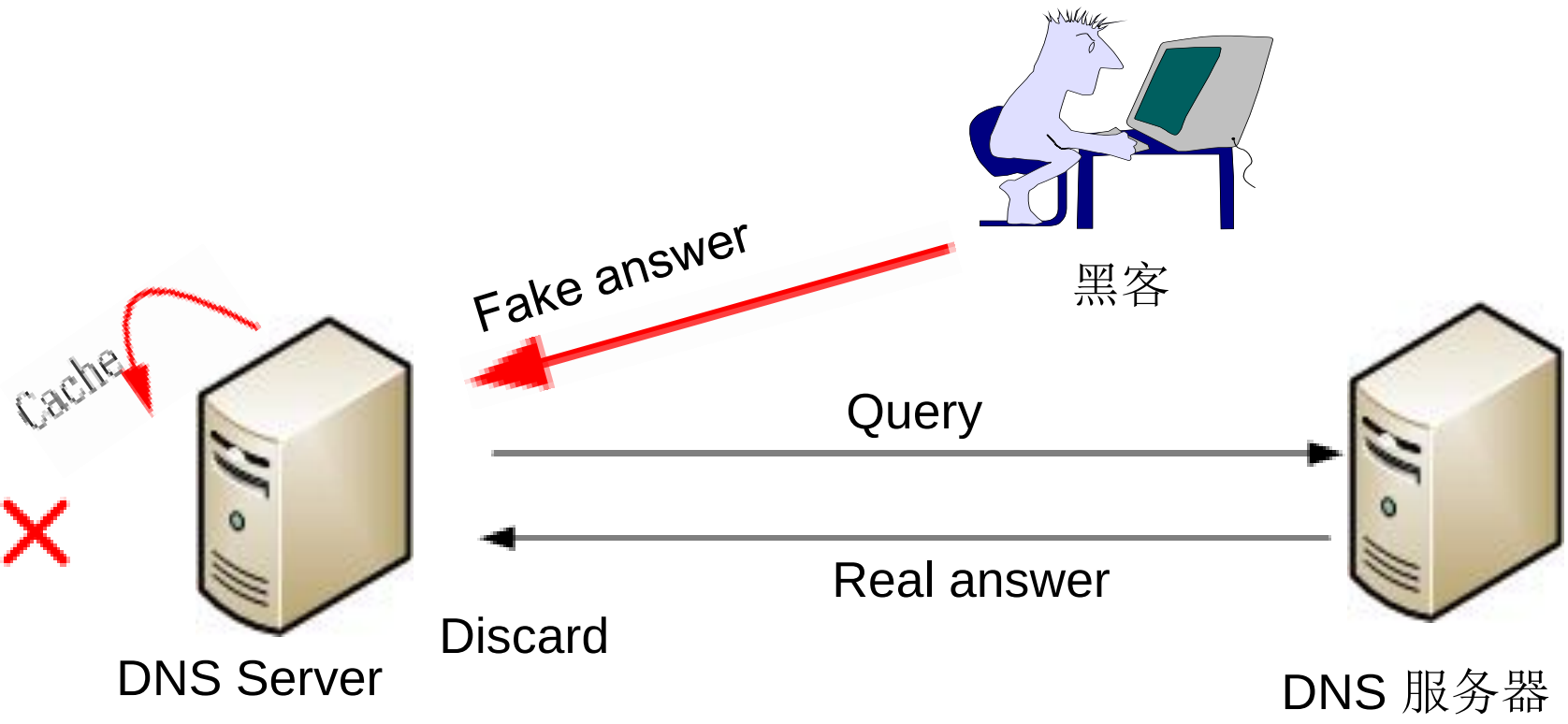
# DNS安全威胁

- DNS欺骗攻击流程



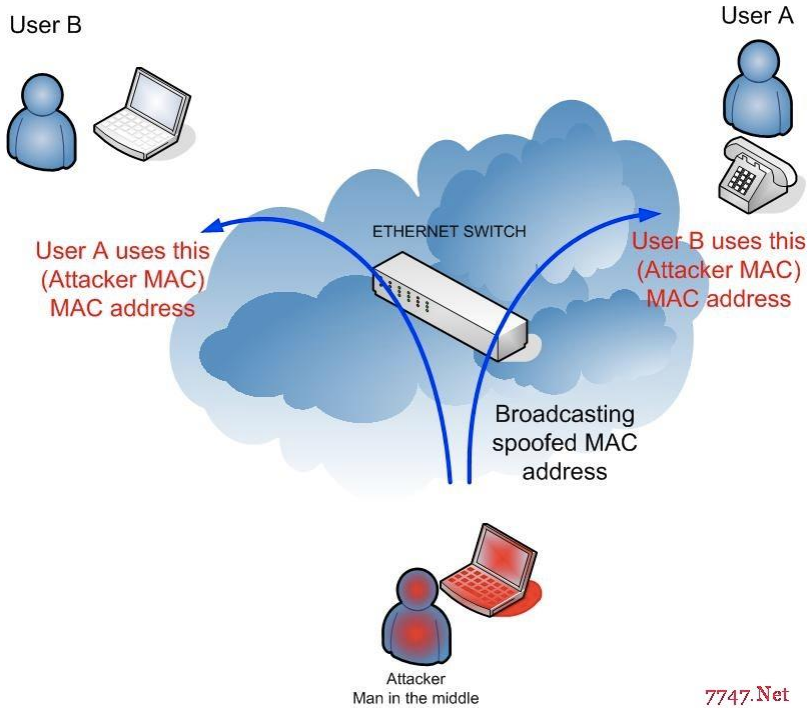
# DNS安全威胁

- DNS下毒攻击流程



# 中间人攻击（Man-in-the-MiddleAttack，“MITM攻击”）

一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。



# GSM网络结构

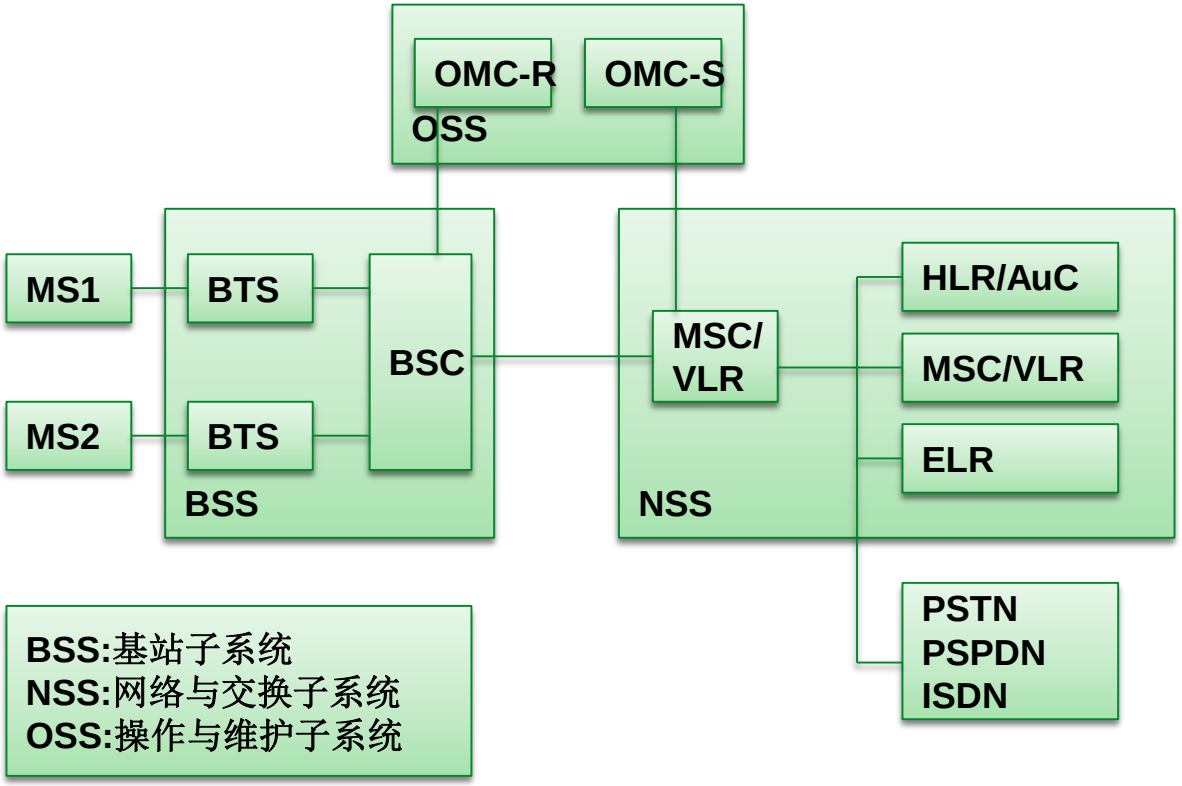
GSM网络主要由以下几个子系统组成：无线子系统(RSS)、网络与交换子系统(NSS)、操作与维护子系统(OSS)。各功能模块如下：

1、**无线子系统(RSS)**
- 移动台(MS)
- 基站子系统(BSS)

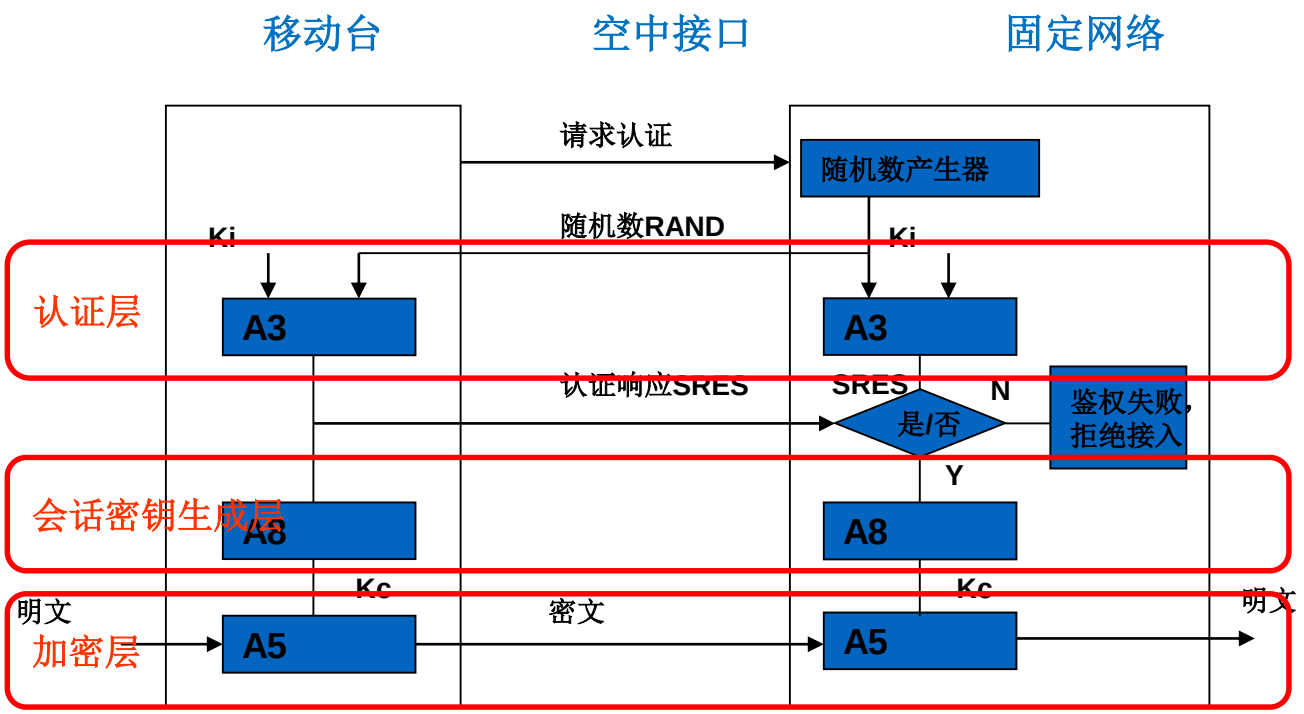
2、**网络与交换子系统(NSS)**
- 移动业务交换中心(MSC)
- 归属位置寄存器(HLR)
- 拜访位置寄存器(VLR)
- 鉴权中心(AuC)
- 设备标识寄存器(EIR)

3、**操作与维护子系统(OSS)**
- 网络与交换子系统操作维护中心(OMC-S)
- 基站子系统操作维护中心(OMC-R)

# GSM网络结构


OMC-R
OMC-S
OSS
MS1
MS2
BTS
BTS
BSC
BSS
MSC/
VLR
NSS
HLR/AuC
MSC/VLR
ELR
PSTN
PSPDN
ISDN
BSS:基站子系统
NSS:网络与交换子系统
OSS:操作与维护子系统

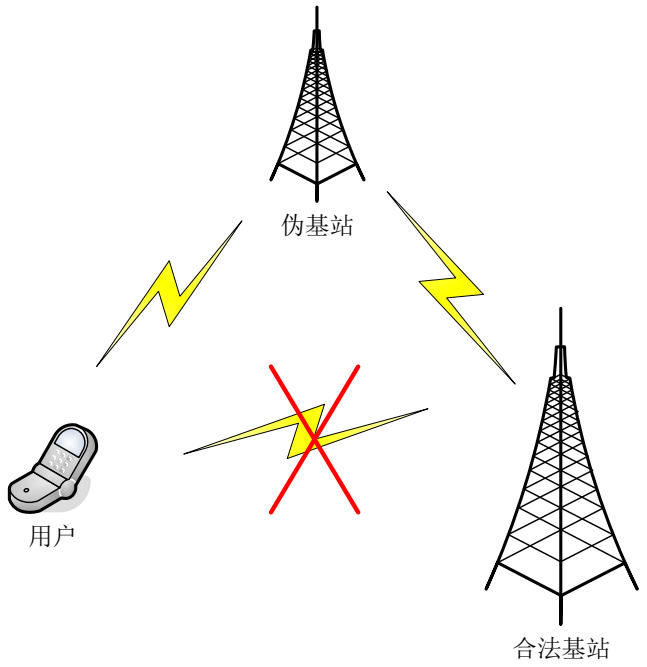
# GSM网络安全体系结构




SRES=A3(RAND,Ki)、 Kc=A8(RAND,Ki)

# 单向鉴权引起的中间人攻击

- 用户身份认证中，GSM只提供了移动网络对移动台的认证，并没有提供移动台对网络的认证。
- 造成危害：
  - 伪基站伪造业务数据
  - 伪基站窃听并篡改业务数据



**身份安全示例——**

# 直接类

## 声音图像视频欺骗/网络终端行为

# AI系统被滥用造成安全问题

- 攻击者使用人工智能技术伪造他人字迹、声音、视频等，真假难辨。

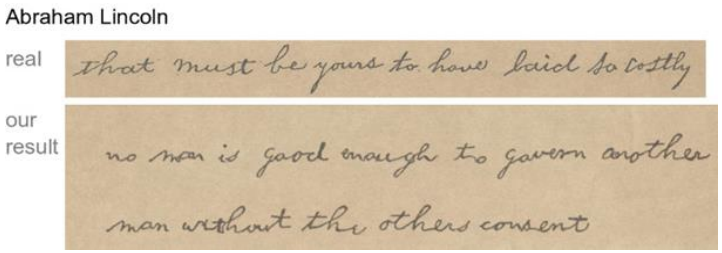
耳听也可能为虚

Natural TTS Synthesis by Conditioning WaveNet on Mel Spectrogram Predictions
J Shen, R Pang, RJ Weiss, M Schuster, N Jaitly... - arXiv preprint arXiv ..., 2017 - arxiv.org

眼见未必为实


Face2face: Real-time face capture and reenactment of rgb videos
J Thies, M Zollhofer, M Stamminger... - Proceedings of the ..., 2016 - cv-foundation.org

AI伪造真人字迹以假乱真




http://visual.cs.ucl.ac.uk/pubs/handwriting/

# 身份认证实例：鼠标用户识别

- 检测原理
  - 在大数据的背景下，利用大量的用户鼠标行为数据提取特征，为用户建立模型；
  - 通过检测一小段使用者的行为数据，与模型匹配，通过识别算法进行判断。

**方法：用户认证方法之一，通过机器学习方法，统计用户使用规律，训练后进行识别，识别算法多样。**

# 身份认证实例：鼠标用户识别

鼠标动作：

用户的鼠标行为基本可以由以下的五个单元行为组成：移动鼠标、按下鼠标左键、抬起鼠标左键、按下鼠标右键、抬起鼠标右键。例如，左键的拖拉行为则由按下鼠标左键、移动鼠标、抬起鼠标左键组成；右键点击由按下鼠标右键、抬起鼠标右键组成。通过综合用户的各种行为，定义了如下四种用户鼠标行为：

- **鼠标移动 Mouse-Move**（MM）表示普通的鼠标移动行为。
- **鼠标拖拉 Drag-and-Drop**（DD）表示鼠标左键或右键的拖动以及拉动行为。
- **鼠标点击 Point-and-Click**（PC）表示鼠标左键或右键的单击、双击行为。
- **静止 Slience** 表示无动作发生。

# 身份认证实例：鼠标用户识别

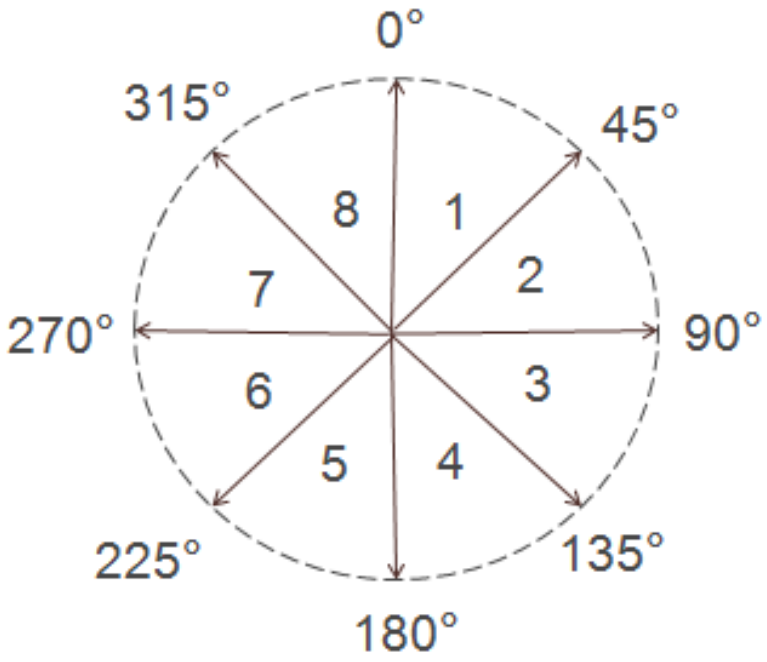
鼠标动作：

| 用户鼠标行为判定 | |
|---|---|
| 按下左键+移动鼠标+抬起左键 | 鼠标拖拉（Drag&Drop） |
| 移动鼠标 | 鼠标移动（MouseMove） |
| 按下左键+抬起左键 | 鼠标点击（Point&Click） |
| 无消息 | 静止Silence |

# 身份认证实例：鼠标用户识别

方向划分：

采用平面上的方向划分方法，将平面的360°均匀地划分为8个方向，编号为1-8，每个方向占45°。



# 身份认证实例：鼠标用户识别

数据规范：

- 采用0.25秒作为最小时间间隔。若鼠标行为持续时间低于最小时间间隔，那么将忽略该行为。

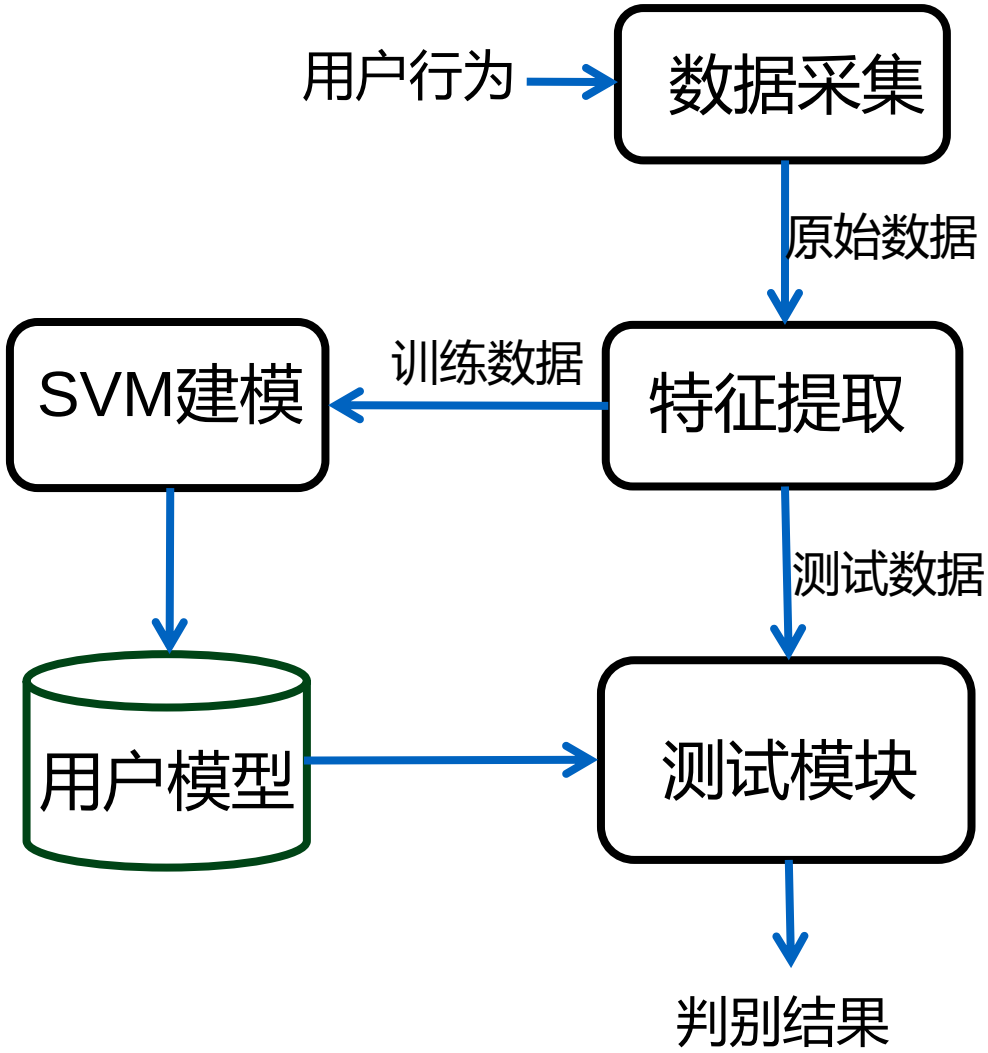
- 位移方面将选取像素点pixels作为用户鼠标行为的位移单位，选取时将过滤掉位移低于25pixels和高于800pixels的用户鼠标行为。

数据采集时往往会产生大量微小的位移行为，称之为抖动数据，这类数据与用户行为特性没有太大关联，存在将会降低系统对用户鼠标行为特性的识别。而位移过大的异常行为发生概率低，也不需要纳入数据分析中，这类数据成为噪音数据。

# 身份认证实例：鼠标用户识别

方案设定：

- 参与人数：21人
- 用户采集时间：24h/人
- 采集系统：Windows
- 操作内容：不限
- 采集结果：数据库表



# 身份认证实例：鼠标用户识别

用户鼠标行为采集结果：

| Column | Type | Default Value | Nullable | Character Set |
|---|---|---|---|---|
| id | int(11) | | NO | |
| event_id | int(11) | | NO | |
| distance | int(11) | | NO | |
| duration | mediumtext | | NO | utf8 |
| speed | float | | NO | |
| direction | int(11) | | NO | |
| start_time | mediumtext | | NO | utf8 |
| end_time | mediumtext | | NO | utf8 |
| user_id | varchar(30) | | NO | utf8 |
| timespan_index | int(11) | | NO | |

(动作类型、距离、持续时间、速度、方向等)

| id | event_id | distance | duration | speed | direction | start_time | end_time | user_id | timespan_index |
|---|---|---|---|---|---|---|---|---|---|
| 175 | 1 | 413 | 625 | 661.... | 5 | 420859 | 421484 | chenyu | 44 |
| 176 | 7 | 0 | 157 | 0 | 0 | 422968 | 423125 | chenyu | 44 |
| 177 | 3 | 48 | 1141 | 42.5... | 5 | 421984 | 423125 | chenyu | 44 |
| 178 | 10 | 0 | 468 | 0 | 0 | 422500 | 422968 | chenyu | 44 |
| 179 | 1 | 368 | 359 | 1025... | 1 | 423828 | 424187 | chenyu | 44 |
| 180 | 1 | 651 | 1156 | 563.... | 3 | 424453 | 425609 | chenyu | 44 |
| 181 | 7 | 0 | 125 | 0 | 0 | 426406 | 426531 | chenyu | 44 |

(部分数据内容)

# 身份认证实例：鼠标用户识别

特征定义:

- **各移动距离的平均操作速度(MSD)** ---表示在不同的距离范围下，用户鼠标行为的平均操作速度，长度为8；
- **各方向的平均操作速度(MDA)** ---表示在不同方向下，用户鼠标行为的平均操作速度，长度为8；
- **各方向的操作数量比例(MDH)** ---表示在不同方向下，用户鼠标行为的数量比例，长度为8；
- **各类型的平均操作速度(ATA)** ---表示在不同鼠标动作类型下，用户操作的平均速度，长度为3；
- **各类型的操作数量比例(ATH)** ---表示在不同鼠标动作类型下，用户的操作数量比例，长度为4；
- **各移动距离的操作数量比例(TDH)** ---表示在不同的距离范围下，用户操作的数量比例，长度为8；
- **各持续时间的操作数量比例(MTH)** ---表示在不同的持续时间范围下，用户操作的数量比例，长度为8；

# 身份认证实例：鼠标用户识别

特征定义:

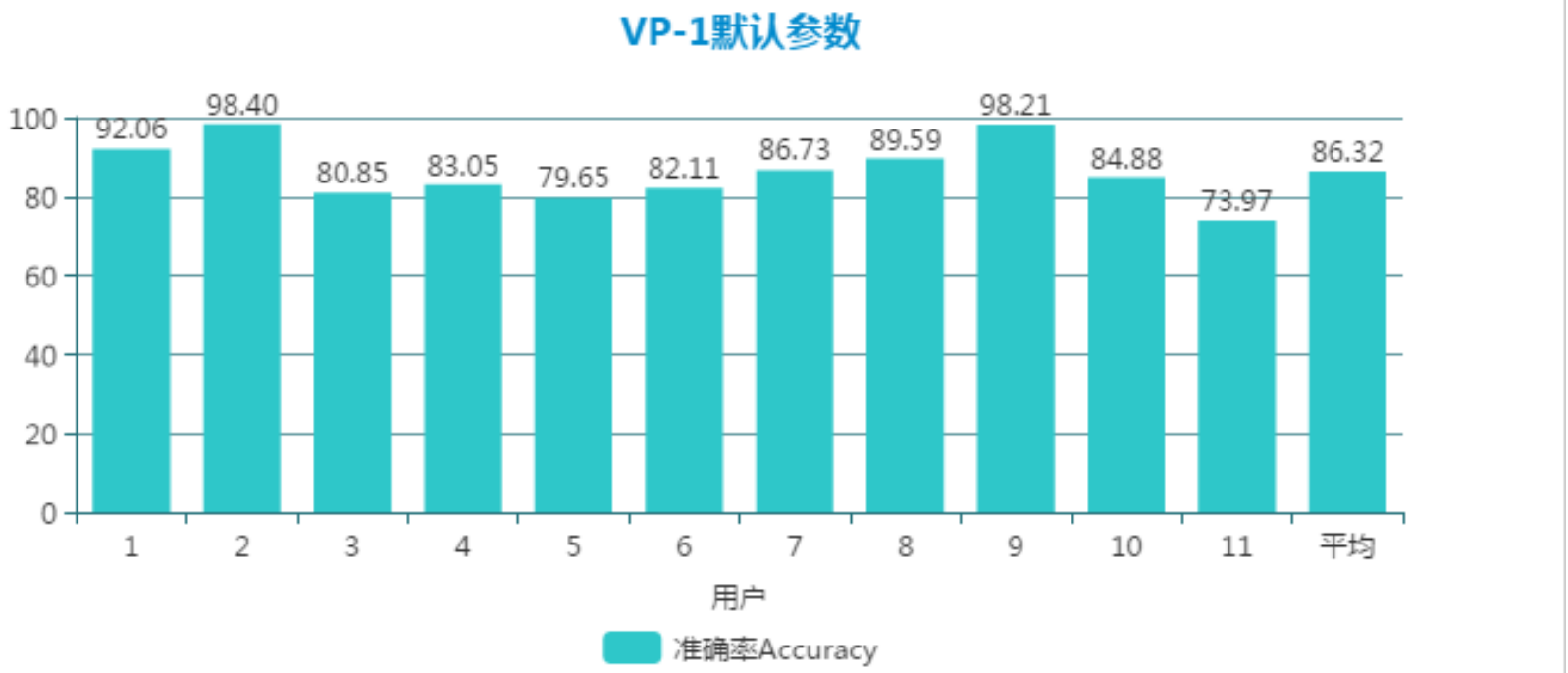
| 特征 | 范围 | 单位 | 长度 |
|---|---|---|---|
| MSD各移动距离的平均操作速度 | 25-800 | 像素/秒 | 8 |
| MDA个方向的平均操作速度 | 25-800 | 像素/秒 | 8 |
| MDH各方向的操作数量比例 | 0-100 | % | 8 |
| ATA各类型的平均操作速度 | 25-800 | 像素/秒 | 3 |
| ATH各类型的操作数量比例 | 0-100 | % | 4 |
| TDH各移动距离的操作数量比例 | 0-100 | % | 8 |
| MTH各持续时间的操作数量比例 | 0-100 | % | 8 |

至此，本项目共选择了7个特征，特征向量长度总共为47。

# 身份认证实例：鼠标用户识别

## 训练模型/测试

SVM模型使用**默认参数**（c=2，g=1）的测试结果：



# 身份认证实例：鼠标用户识别

国外实验：

- Lin [6]通过微软电脑下用户的每日鼠标互动数据，设计了一个持续认证系统。系统将11个志愿者的鼠标行为数据分为三个样例集合。集合A包含了在Windows Explorer下用户完成文件相关操作的鼠标动作的特征向量。作为对比，集合B包含了在Windows Explorer下用户的鼠标动作的特征向量，而集合C则包含了用户使用电脑时的全部鼠标动作的特征向量。如同他们设想的一样，最好的结果来自于数据集合A，因为用户在文件相关操作下往往使用相似的方法，因此用户的动力学特征更具一致性。

- Shen [7]则基于鼠标交互设计了一个持续的认证系统。这个系统不需要非法入侵者的测试数据。该系统基于28个用户的鼠标行为数据，侧重于不同的鼠标事件、鼠标操作以及鼠标行为模式，并使用了不同的分类器进行分类。最后，该系统通过一级支持向量机探测器得到了FMR为0.37%、FNMR为1.12%的最佳结果。

# 问题和讨论