第二部分　访问控制

02.　生物认证

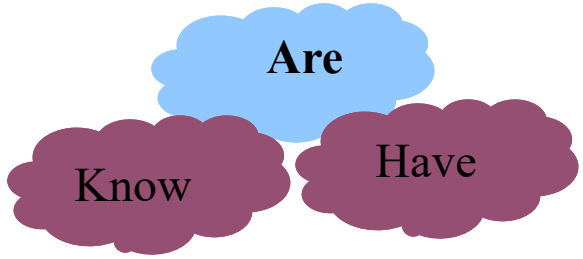
厚 德 健 行

你本身的特征

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 生物统计学
  - “你就是你的密钥” —— Schneier

  - 例如
    - 指纹
    - 脸部识别
    - 语音识别
    - 步态识别
    - 虹膜
    - 更多!



为何选择生物统计学认证?

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 作为密码更安全的代替
- 需要一种便宜可靠的生物统计学认证方法
  - 目前，基于生物统计学的认证方法是一个热门领域
- 基于生物统计学的认证在安全领域的应用
  - 拇指指纹鼠标
  - 掌纹识别系统
  - 指纹识别仪
  - 人脸识别门禁系统
  - 语言登录系统

理性的基于生物统计学的认证特征

- 通用性 — 几乎能应用于每个人
  - 实际上, 没有一个基于生物统计学的认证能用于每个人
- 区分性 — 能区分确定的事物
  - 实际上, 不能希望100%的确定
- 持久性 — 生物特征应永远不会变
  - 实际上, 特征在一段合理的时间内不变就足够了
- 可收集性 — 物理特征应该很容易收集
  - 在很大程度上依赖于对象是否合作
- 安全性、易用性，等等.

基于生物统计学的模式

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 鉴定 — 谁能去做?
  - 比较是一对多的
  - 例如: FBI指纹数据库
- 认证 — 真的是你吗?
  - 比较是一对一
  - 例如: 拇指指纹鼠标
- 鉴定的问题更加复杂
  - 因为存在更多的比较，所以匹配更为随机
- 本节主要讨论认证问题

登记 vs 识别

- 登记阶段
  - 首先将对象的生物信息输入到数据库
  - 必须小心地检测相关的生物信息
  - 处理过程慢一点和进行多次测量都是可以接受的
  - 生物信息必须是精确的，这样利于识别
  - 在已使用的系统中，登记被证明是一个弱点
- 识别阶段
  - 将生物测试系统用到实际中
  - 必须迅速、简单和精确

合作对象

- 假设对象是合作的
- 对于鉴定问题，对象通常是不合作的
- 例如：面部识别
  - 拉斯维加斯赌场被建议使用该系统来监测有名的骗子（也被建议用来在机场监测恐怖分子等）
  - 但登记条件离理想状态较远
  - 识别阶段，对象不合作，他们将尽可能地逃离监测
- 合作的对象使生物问题更加容易
  - 我们关注认证阶段，
  - 所以，对象是一般合作的

错误的类型

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 误报率 vs 漏报率
  - 误报 — 用户B被错误的认证为了A
  - 漏报 — 用户A不被认证为A
- 对于任何生物测定，都可以降低误判率或拒判率，但往往是以牺牲另一个为代价
- 例如：
  - 声纹匹配门槛为99% ⇒ 低误报率，高漏报率
  - 声纹匹配门槛为30% ⇒ 高误报率，低漏报率
- 相等错误率: 指误报率和漏报率相同的概率
  - 当进行不同生物系统比较时，这是个很有用的度量标准

指纹的历史

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 1823 — Johannes Evangelist Purkinje讨论了9种指纹模式
- 1858 — 印度William Hershel爵士使用掌纹和指纹作为合同的一种签名形式
- 1880 — Henry Faulds医生在Nature上发表论文，指出指纹有作为鉴定的用途
- 1883 — Mark Twain的小说《密西西比河上的生活》中，一个谋杀者通过指纹被鉴定出来

指纹的历史

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 1888 — Francis Galton爵士(达尔文的堂兄)提出了分类系统
  - 目前，基于”细节“的分类系统仍在使用
  - 也验证了指纹特征是不变的
- 指纹已广泛地用于鉴定，特别是用于犯罪的场合
  - 在英国，指纹必须有16个解或点是匹配的
  - 在美国，则没有固定的数目要求

指纹的比较

- 指纹纹路的环状、涡纹、拱形
- 从图像中提取细节

环状 (双)

涡纹

拱形

指纹特征自动提取

- 捕获指纹的图像
- 增强图像
- 鉴定细节

指纹特征

- 增强图像中细节和存入数据库中的用户细节进行比较
- 这是统计学匹配吗?
- 旁白：同卵双胞胎指纹的不同呢？

手掌几何图形

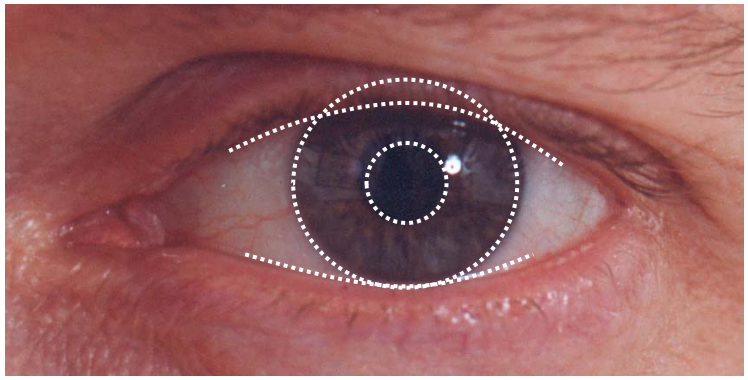
- 流行的生物测定形式
- 手的形状被确切的测量
  - 手掌与手指的宽度
  - 手指的长度等
- 人类的手并不是独一无二的
- 手的几何图形测量快速
- 但对于个人身份认证不太适用

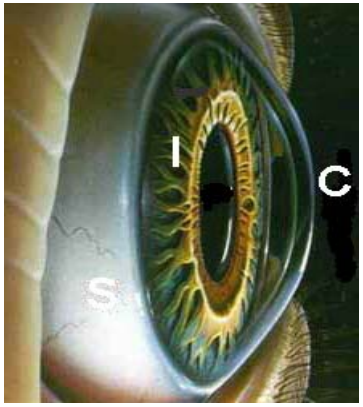
手掌几何图形

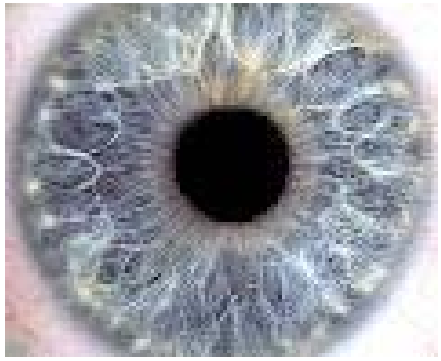
浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 优点
  - 处理速度迅速----登记阶段需要不到1分钟，识别阶段也不到5秒钟
  - 手掌是对称的，那又怎么样呢？
- 缺点
  - 不能用于年轻人或非常老的人
  - 相对高的相等错误率

虹膜模式







- 虹膜的生成是混乱无序的
- 没有或有较少的遗传影响
- 甚至在孪生子中也不相同
- 虹膜的模式一生都是不变的

虹膜识别的历史

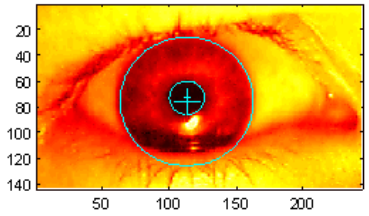
浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

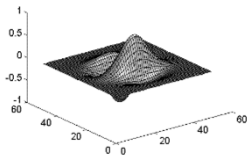
- 1936 — Frank Burch提出的
- 1980s — James Bond的电影重新提出
- 1986 — 第一个专利才出现
- 1994 — John Daugman将目前被认为是最好的虹膜扫描方法申请了专利
  - Iridian技术公司拥有该专利

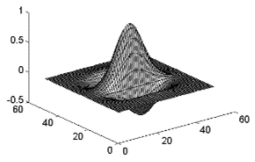
虹膜扫描

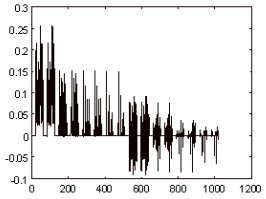
浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

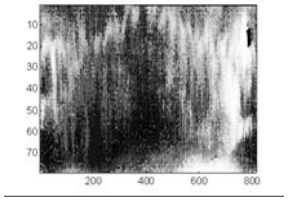
- 扫描仪首先定位虹膜
- 然后对眼睛拍黑白照
- 做二维小波变换处理
- 得出256字节的”虹膜代码“











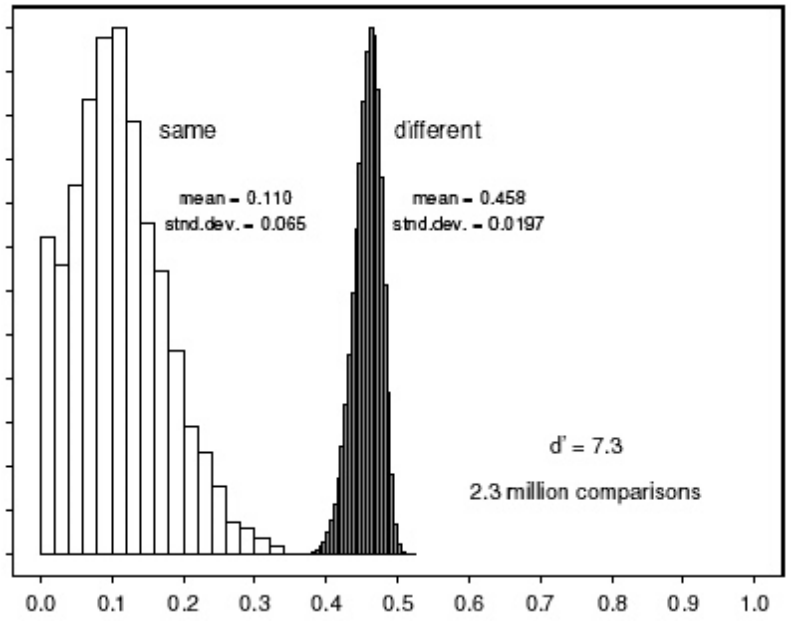
测量虹膜的相似性

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 基于代码间的汉明距离
- d(x,y)定义为
  - 未匹配的位数/比较的位数
  - 如：d(0010,0101) = 3/4 和 d(101111,101001) = 1/3
- d(x,y)用2048位虹膜代码计算
  - 一个完美的匹配对应的d(x,y) = 0
  - 实验室条件下同样的虹膜期望距离是0.08
  - 随机情况下，期望距离为0.50
  - 通常的阈值0.32。当小于0.32时，比较匹配；否则，不匹配

虹膜扫描错误率

距离	误判率
0.29	1 in $1.3*10^{10}$
0.30	1 in $1.5*10^{9}$
0.31	1 in $1.8*10^{8}$
0.32	1 in $2.6*10^{7}$
0.33	1 in $4.0*10^{6}$
0.34	1 in $6.9*10^{5}$
0.35	1 in $1.3*10^{5}$



距离

相等错误率

对虹膜扫描系统的攻击

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 一张清晰的眼睛扫描照片
  - 攻击者可能使用该照片去欺骗系统认证

- 曾有个阿富汗妇女由照片提取的虹膜通过了系统认证
- 为了避免这种攻击，某些虹膜扫描系统首先会在拍照前将一束光打到眼睛上来验证瞳孔

相等错误率比较

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 相等错误率(EER): 误判率==拒判率
- 指纹系统 相等错误率约为5%
- 手掌图形系统相等错误率为10^{-3}
- 理论上, 虹膜扫描 的相等错误率约10^{-6}
  - 但实际上这一目标是难以实现的
  - 登记阶段必须非常精确
- 实际上，很多其他生物测定法比指纹法更为糟糕
- 基于生物统计学的认证比较有用
  - 但是对于鉴定这一问题，生物统计学的认证方法今天用的很少

生物统计学: 底线

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

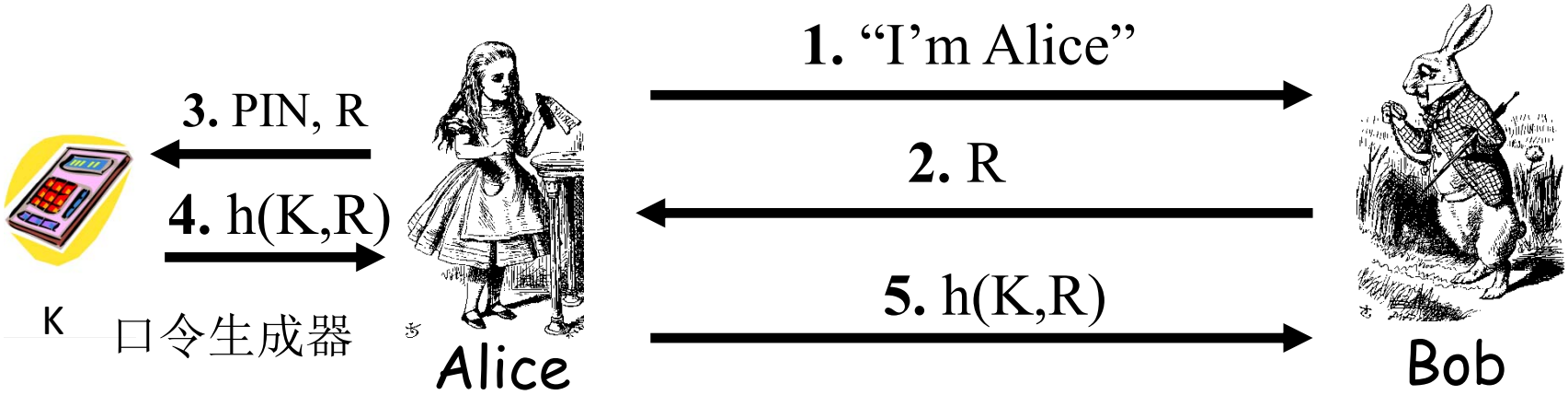
- 基于生物统计学的认证方法难以伪造
- 但攻击者可以
  - 偷取Alice的指纹
  - 使用Bob的指纹副本
  - 破坏进行比较的软件或修改包括登记数据的数据库等
- 被破译的生物特征被废除或替换?
- 基于生物统计学的认证的安全性存在问题!
- 基于生物统计学的认证至今没有被广泛的使用
- 这种局面将会改变

你所拥有的

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 你所拥有的
- 例如
  - 车钥匙
  - 手提电脑（或它的MAC地址）
  - 口令生成器
  - ATM卡,智能卡

口令生成器



- Bob发送一个随机的”质询“(challenge)信息R给Alice
- Alice将R和PIN码输入到口令生成器中
- 用口令生成器对对称密钥K和R进行hash
- Alice将一个应答结果h(K,R) 发送回给Bob
- Bob验证应答
- 注意：Alice拥有口令生成器和已知的PIN码

双因素认证

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 需要使用3种认证方法中的两个：
  1. 你所知道的
  2. 你所拥有的
  3. 你本身的特征
- 例如：
  - ATM卡: 卡和PIN码
  - 信用卡: 卡和签名
  - 口令生成器:设备和PIN码
  - 需要口令的生物指纹鼠标和有PIN码的智能卡

单点登录

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 用户发现重复输入认证信息非常麻烦
  - 用户的登录仅需要认证一次
  - 让用户的“信任状”伴随着他们访问Intenet
  - 以后的认证对于用户来说就是透明的
- 安全认证系统----例如单点登入协议
- Internet上的单点登录?
  - 微软:”身份验证” **(Passport)**
  - 其他方法:”自由联盟“(**Liberty Alliance)**
  - 基于声明标记语言(**SAML**)

Web Cookies

浙江工业大学 ZHE JIANG UNIVERSITY OF TECHNOLOGY

- 网站提供给用户一个web cookie，它仅是存放在用户的电脑上并被用户浏览器管理的简单数值
- 网站采用cookie值作为查询数据库的索引
- Cookie通过会话(session)来维持状态
  - Web采用无状态的协议: HTTP
  - Cookie同样拥有保留session中的状态
- 从某种意义看，cookie可以看做站点的单点登录方法
  - 通过一种非常弱的认证模式
- Cookie和隐私问题

关注我，下节内容更精彩：

03. 隐通道、推理控制和captcha