第六讲：身份认证

一、身份认证的基本概念

二、通行字认证系统

身份认证

身份认证：在一个有竞争和争斗的现实社会中，身份欺诈是不可避免的，因此常常需要证明个人的身份。 传统的身份认证一般靠人工的识别，正逐步由机器代替。在信息化社会中，随着信息业务的扩大，要求验证的对象集合也迅速加大，因而大大增加了身份验证的复杂性和实现的困难性。

身份认证的基本概念

- **身份认证必要性**：在一个有竞争和争斗的现实社会中，身份欺诈是不可避免的，因此常常需要证明个人的身份。通信和数据系统的安全性也取决于能否正确验证用户或终端的个人身份。
- **传统的身份认证**：一般是通过检验“物”的有效性来确认持该物的的身份。“物”可以为徽章、工作证、信用卡、驾驶执照、身份证、护照等，卡上含有个人照片 (易于换成指纹、视网膜图样、牙齿的X适用的射像等) ，并有权威机构签章。这类靠人工的识别工作已逐步由机器代替。
- **信息化社会对身份认证的新要求**：随着信息业务的扩大，要求验证的对象集合也迅速加大，因而大大增加了身份验证的复杂性和实现的困难性。实现安全、准确、高效和低成本的数字化、自动化、网络化的认证。

身份认证的基本概念

1. 身份欺诈的方式

(1) 象棋大师问题。

A不懂象棋，但可向 G. Kasparov 和A. Karpov 同时挑战，在同一时间和地点进行 (不在一个房子) 对弈，以白子棋对前者以黑子棋对后者，而两位大师彼此不通气，参看如下示图。Karpov 持白子棋先下一步，A记下走到另一房下同样一着，而后看 Kasparov 如何下黑子棋，A记下这第二步对付 Karpov，以此类推。这是一种**中间人欺诈**。

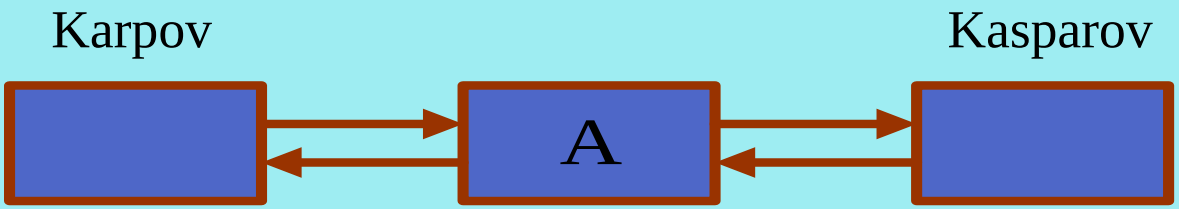

图1 象棋大师问题

身份认证的基本概念

(2) The Mafia欺诈。

A在Mafia集团成员B开的饭馆吃饭，Mafia集团另一成员C到D的珠宝店购珠宝，B和C之间有秘密无线通信联络，A和D不知道其中有诈。A向B证明A身份并付账，B通知C开始欺骗勾当，A向B证明身份，B经无线通知C，C以同样协议与D实施。当D询问C时，C经B向A问同一问题，B再将A的回答告诉C，C向D回答，参看图。实际上，B和C起到中间人作用完成A向D的身份认证，实现了C向D购买了值钱珠宝，而把账记在A的账上。这是中间人B和C合伙进行的欺诈。

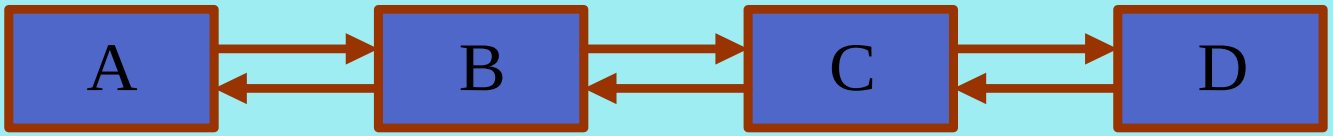

图2 中间人合伙欺诈

身份认证的基本概念

(3) 恐怖分子欺诈

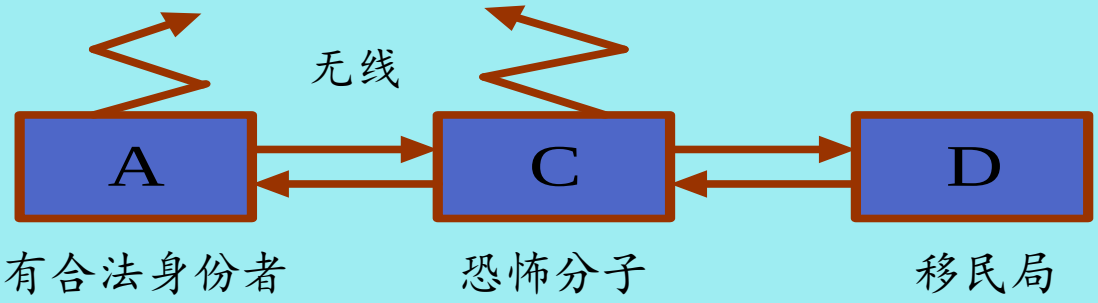

图3 另一种中间人合伙欺诈

假定C是一名恐怖主义者，A要帮助C进入某国，D是该国移民局官员，A和C之间有秘密无线电联络。A协助C得到D入境签证。这类欺诈可以用防电磁幅射泄露和精确时戳等技术来抗击。

(4) 多身份欺诈 (Multiple identity frand)： A首先建立几个身份并公布之。其中之一他从来未用过，他以这一身份作案，并且只用一次，除目击者 (Witness) 外无人知道犯罪人的个人身份。由于A不再使用此身份，而无法跟踪。采用一种机构，且每人只能有一个身份认证就可抗击这类欺诈。

身份认证的基本概念

2. 身份认证系统的组成和要求

组成：

- **示证者**P (Prover)，出示证件的人，又称作申请者 (Claimant)，提出某种要求；
- **验证者**V (Verifier)，检验示证者提出的证件的正确性和合法性，决定是否满足其要求；
- **攻击者**，可以窃听和伪装示证者骗取验证者的信任。
- **可信赖者**，参与调解纠纷。必要时的第四方。

身份认证的基本概念

身份认证技术，又称作**识别** (Identification)、**实体认证** (Entity authentication)、**身份证实** (Identity verification) 等。实体认证与消息认证的差别在于，消息认证本身不提供时间性，而实体认证一般都是实时的。另一方面实体认证通常证实实体本身，而消息认证除了证实消息的合法性和完整性外，还要知道消息的含义。

对身份认证系统的要求：

(1) 验证者正确识别合法示证者的概率极大化。

(2) 不具可传递性 (Transferability)，验证者B不可能重用示证者A提供给他的信息来伪装示证者A，而成功地骗取其他人的验证，从而得到信任。

身份认证的基本概念

(3) 攻击者伪装示证者欺骗验证者成功的概率要小到可以忽略的程度，特别是要能抗已知密文攻击，即能抗攻击者在截获到示证者和验证者多次 (多次式表示) 通信下伪装示证者欺骗验证者。

(4) 计算有效性，为实现身份认证所需的计算量要小。

(5) 通信有效性，为实现身份认证所需通信次数和数据量要小。

(6) 秘密参数能安全存储。

(7) 交互识别，有些应用中要求双方能互相进行身份认证。

(8) 第三方的实时参与，如在线公钥检索服务。

(9) 第三方的可信赖性。

(10) 可证明安全性。

身份认证的基本概念

3. 身份认证的基本分类

- **身份证实** (Identity Verification) 要回答**你是否是你所声称的你?** 即只对个人身份进行肯定或否定。一般方法是输入个人信息，经公式和算法运算所得的结果与从卡上或库中存的信息经公式和算法运算所得结果进行比较，得出结论。

- **身份识别** (Identity Recognition) 要回答**我是否知道你是谁?** 一般方法是输入个人信息后，经处理提取成模板信息，试着在存储数据库中搜索找出一个与之匹配的模板，而后给出结论。例如，确定一个人是否曾有前科的指纹检验系统。

  显然，身份识别要比身份认证难得多。

身份认证的基本概念

4. 实现身份认证的基本途径

身份认证可以依靠下述三种基本途径之一或它们的组合实现。

- **所知** (Knowledge)，个人所知道的或所掌握的知识，如密码、口令等。
- **所有** (Possesses)，个人所具有的东西，如身份证、护照、信用卡、钥匙等。
- **个人特征** (Characteristics)，如指纹、笔迹、声纹、手型、脸型、血型、视网膜、虹膜、DNA以及个人一些动作方面的特征等。

身份认证的基本概念

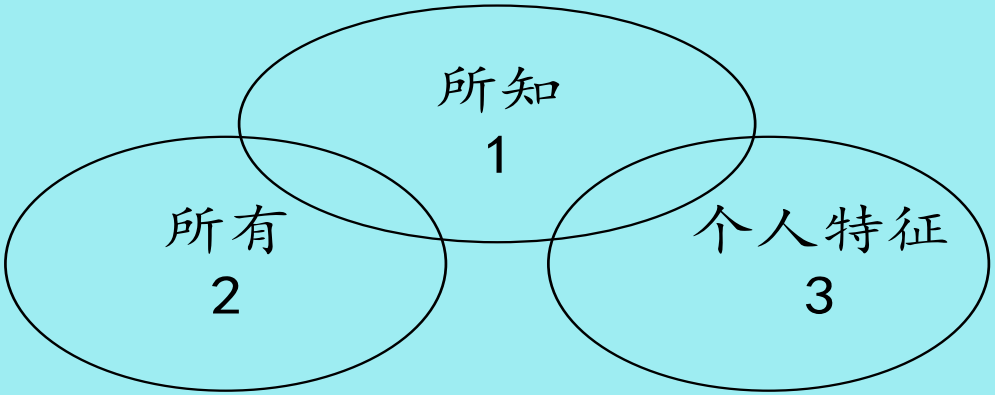

图4 身份认证的基本途径

根据安全水平、系统通过率、用户可接受性、成本等因素，可以选择适当的组合设计实现一个自动化身份认证系统。

身份认证的基本概念

身份认证系统的质量指标

- **拒绝率** FRR (False Rejection Rate) 或**虚报率 (I型错误率)**：合法用户遭拒绝的概率。
- **漏报率** FAR (False Acceptance Rate) **(II型错误率)**：非法用户伪造身份成功的概率。

为了保证系统有良好的服务质量，要求其型错误率要足够小；为保证系统的安全性，要求其型错误率要足够小。这两个指标常常是相悖的，要根据不同的用途进行适当的折中选择，如为了安全 (降低FAR)，则要牺牲一点服务质量 (增大FRR)。设计中除了安全性外还要考虑经济性和用户的方便性。

通行字认证系统

1. 概述

通行字 (也称**口令**、**护字符**) 是一种根据已知事物验证身份的方法，也是一种最广泛被研究和使用的身份验证法。如中国古代调兵用的虎符、阿里巴巴打开魔洞的“芝麻”密语、军事上采用的各种口令以及现代通信网的接入协议。

通行字选择原则：① 易记；② 难以被别人猜中或发现；③ 抗分析能力强。

在实际系统中需要考虑规定选择方法、使用期限、字符长度、分配和管理以及在计算机系统内的保护等。在一般非保密的联机系统中，**多个用户可共用一个通行字**。要求的安全性高时，**每个用户需分别配有专用的通行字**。在要求较高的安全性时，可采用**随时间而变化的一次性通行字**。

通行字认证系统

防止泄露是系统设计和运行中的关键问题。一般，通行字及其响应在传送过程中均要加密，而且常常要附上业务流水号和时戳等，以抗击重放攻击。

为了避免被系统操作员或程序员利用，个人身份和通行字都不能以明文形式在系统中心存放。可用软件进行加密处理。

一个更好的办法是采用**通行短语** (Pass Phrases) 代替通行字，通过**密钥碾压** (Key Crunching) 技术，如杂凑函数，可将易于记忆的足够长的短语变换为较短的随机性密钥。

分发通行字的安全性是极为重要的一环。

通行字可由用户个人选择，也可由系统管理人员选定或由系统自动产生。

通行字认证系统

2. 通行字的控制措施

(1) 系统消息 (System Message)。一般系统在联机和脱机时都显示一些礼貌性用语，而成为识别该系统的线索，因此这些系统应当可以抑制这类消息的显示。

(2) 限制试探次数。不成功送口令一般限制为3～6次，超过限定试验次数，系统将对该用户ID锁定。

(3) 通行字有效期。限定通行字的使用期限。

(4) 双通行字系统。允许联机用通行字，和允许接触敏感信息还要送一个不同的通行字。

(5) 最小长度。限制通行字至少为6～8个Bytes 以上，防止猜测成功概率过高，可采用**掺杂** (Salting) 或采用**通行短语**等加长和**随机化**。

通行字认证系统

(6) 封锁用户系统。可以对长期未联机用户或通行字超过使用期的用户的ID封锁。直到用户重新被授权。

(7) 根通行字的保护。根 (Root) 通行字是系统管理员访问系统所用口令，由于系统管理员被授予的权利远大于对一般用户的授权，因此它自然成为攻击者的攻击目标。因此在选择和使用中要倍加保护。要求必须采用16进制字符串、不能通过网络传送、要经常更换 (一周以内) 等。

(8) 系统生成通行字。有些系统是不允许用户自己选通行字，而由系统生成、分配通行字。系统如何生成易于记忆又难以猜中的通行字是要解决的一个关键问题；另一危险是若生成算法被窃，则危及整个系统的安全。UAX IVM S V.4.3系统能保证所产生的通行字具有可拼读性。

通行字认证系统

3. 通行字的检验

- **反应法** (Reactive)：利用一个程序 (Cracker)，让被检通行字与一批易于猜中的通行字表中成员进行逐个比较。如果都不相符则通过。这类反应检验法有些缺点：① 检验一个通行字太费时，试想一个攻击者可能要用几小时甚至几天来攻击一个通行字。②现用通行字都有一定的可猜性，但直到采用反应检验后用户才更换通行字。
- **支持法** (Proactive)：用户先自行选一个通行字，当用户第一次使用时，系统利用一个程序检验其安全性，如果它易于被猜中，则拒绝并请用户重新选一个新的。通过准则要考虑可猜中性与安全性的之间的折衷，若算法太严格，则用户所选通行字屡遭拒绝而招致用户报怨。另一方面如果很易猜中的通行字也能通过，则影响系统的安全性。

thank you