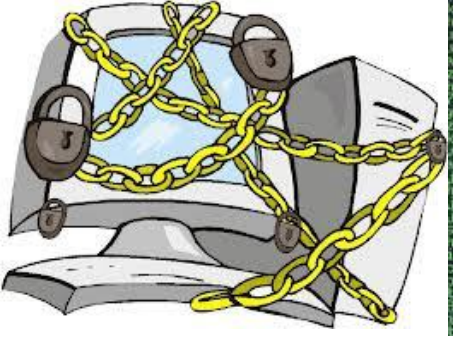



信息系统安全

数据与系统安全保护

身份认证与访问控制

陈春华 博士
chunhuachen@scut.edu.cn

2018 春季
华南理工大学 软件学院

鉴别服务与身份认证

- 鉴别服务
  - 通过对于通信的对等实体（主体）和数据源的鉴别和确认来对抗假冒性攻击以及重放性攻击
  - 网络层鉴别-主机地址鉴别
  - 传输层鉴别-进程地址鉴别
  - 应用层鉴别-人员账户鉴别

大纲

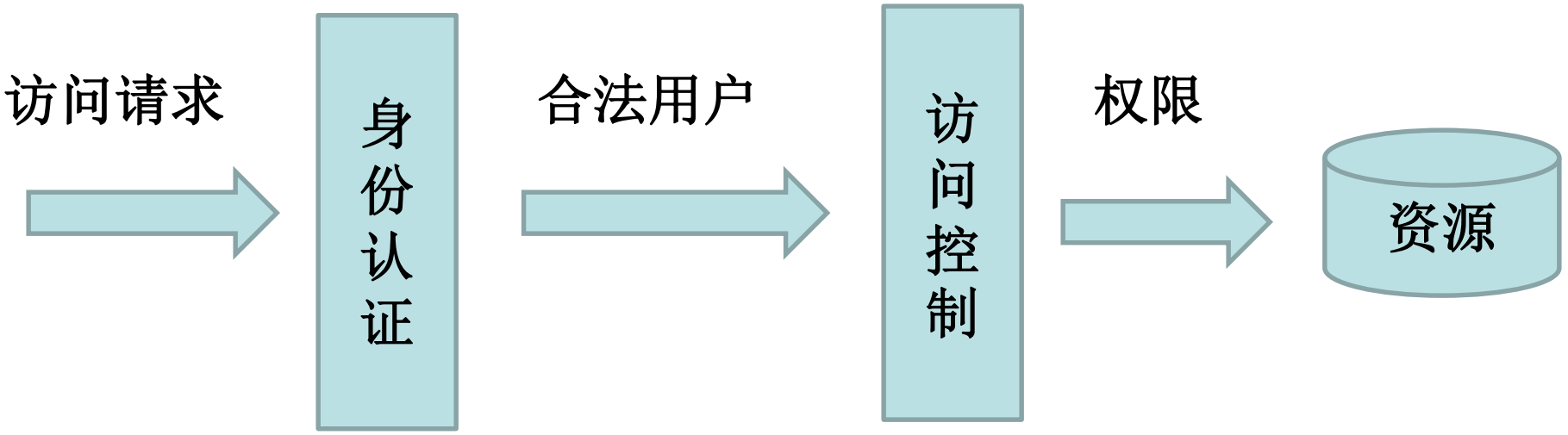
- 基于凭证对比的身份认证
  - 口令认证等
- 基于密钥分发的身份认证
  - 私钥与公钥认证协议（见安全协议）
- 基于数字证书的身份认证
  - X.509数字证书与PKI（见Web安全）
- 信息系统访问授权
  - 自主、强制访问控制

身份认证与访问控制

- 为了系统的安全，需要对（系统）访问进行管制约束。
- 访问涉及两个方面：
  - 主体，通常指用户
  - 客体，也称资源，即数据
- 身份认证是指对主体合法性的认证
- 访问控制是指对于主体的访问行为进行授权的过程

身份认证与访问控制模型

- 不同的合法用户，可能具有不同的权限



基于凭证比对的身份认证

- 用户提交能代表身份的凭证与系统中存储的凭证进行对比。
- 身份凭证主要包括如下3类：
  - 用户所知道的密码，如口令，个人识别号PIN和密钥等
  - 用户所拥有的信物，如信用卡，IC卡，USB Key等
  - 用户自身的生物特征，如指纹，虹膜纹等
- 单因素、双因素认证

静态口令

- 使用度最高的一类身份认证机制
  - 账户公开，口令保密
  - 简单，易用，效率很高，但是极为脆弱，容易受到攻击
- 攻击：
  - 在线暴力猜测、字典猜测
  - 针对口令文件的非在线暴力猜测与字典猜测
  - 网络窃听，键盘记录器，还有社交工程等

静态口令

- 安全保护
  - 口令选择：1) 扩大口令的字符空间，2) 选择长口令，3) 不同系统使用不同的口令
  - 正确使用口令：1) 经常更换口令，2) 限制登录时间等，比如上班时间才能登录
  - 安全保护口令：不存储明文，而是哈希值
  - 其他等

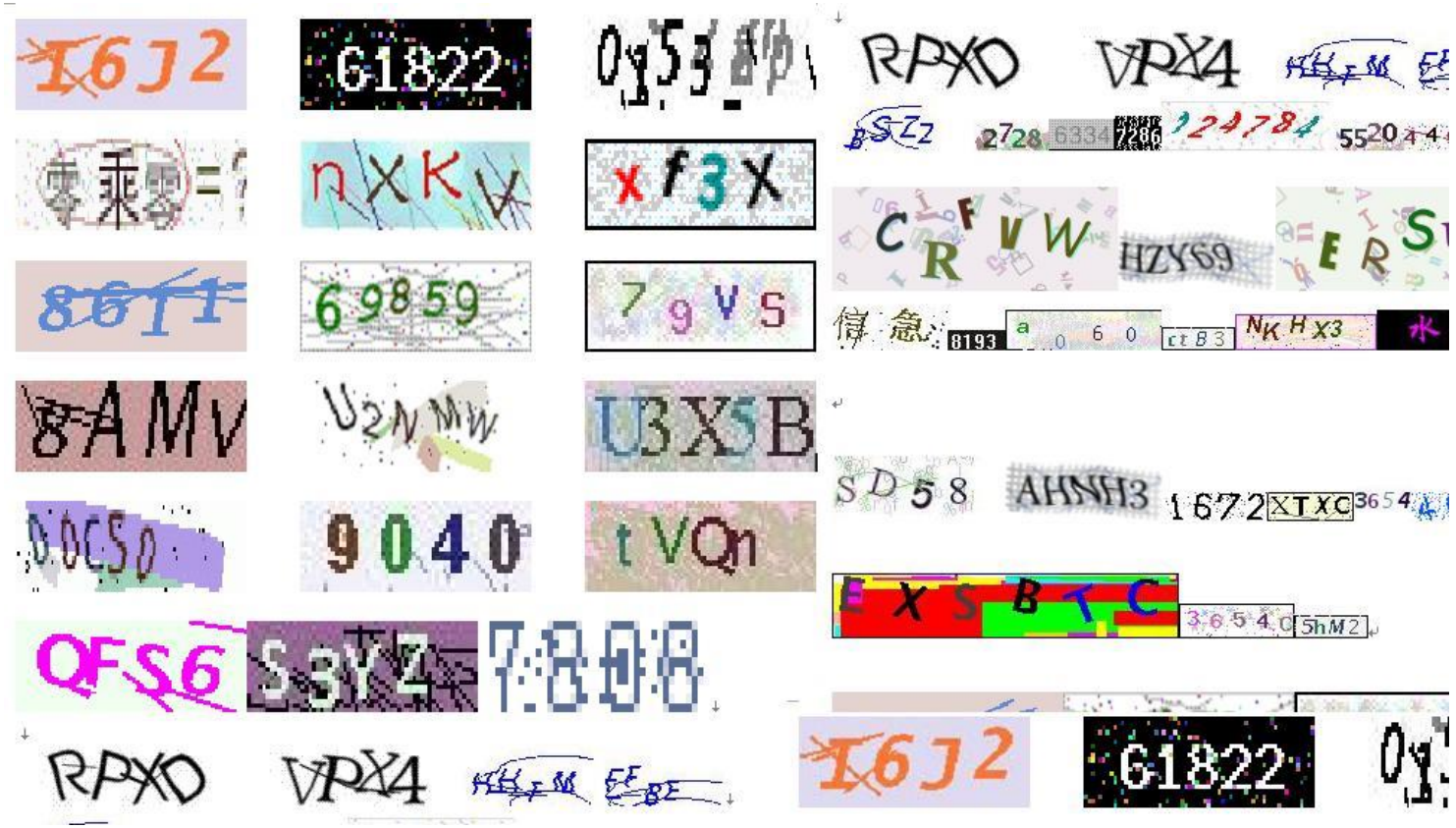
实验@暴力破解Wifi密码(演示)

- 时间，待安排

批量登录攻击与验证码

- 批量登录攻击，即在线暴力破解
- 验证码，也称CAPTCHA，全自动区分计算机和人类的图灵测试
- 强制用户在登录时进行人工操作，通常需要用户从模糊的图形之中辨认出隐藏在其中的一些信息。
- 验证码通常随机生成，并具有一定的生存周期。

验证码示例@互联网

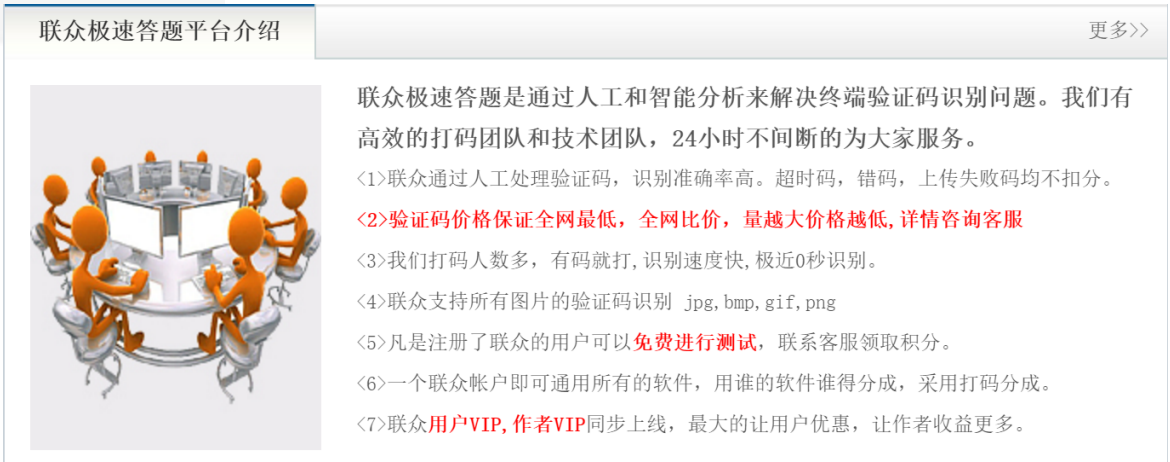

I6J2
61822
RPXD
VPX4
nXKW
xf3X
69859
7 9 V S
8AMV
U2NMW
UBXSB
SD58
AHNH3
1672XTXC
9040
tVQn
QFS6
7808
RPXD
VPX4
I6J2
61822

验证码示例@12306

果壳网: http://www.guokr.com/article/440997/?page=4

破解验证码

- 图像识别，需要很高的人工智能
- 人工打码平台



reCAPTCHA与古籍识别

- CMU-卡内基梅隆大学，设计了一个名叫reCAPTCHA的强大系统，让他们的电脑去向人类求助。
- 具体做法是：将OCR软件无法识别的文字扫描图传给世界各大网站，用以替换原来的验证码图片
- 那些网站的用户在正确识别出这些文字之后，其答案便会被传回CMU。
- 将古籍转化为电子文档~~~
- Facebook参与其中？

Review@2016/03/17

- 鉴别服务与身份认证(应用层)
  - 基于凭证的对比
    - 口令：静态和动态

- 鉴别/认证: 将请求用户与系统合法用户绑定的过程；在这个过程中，请求者提交认证参数供系统进行验证。
- 认证通过的用户，还需经过授权的过程才能使用系统的保护资源。

动态口令

- 又称为一次性口令，是最安全的口令。
- 它根据专门的算法生成一个不可预测的随机数字组合，每一个密码只能使用一次。
  - 通常由专门的口令生成器生成，又称令牌
  - 包括，短信密码，手机令牌，硬件令牌等
- 广泛运用在网上银行，电子商务等场景。
  - 6位的数字验证码

动态口令

- 生成动态口令的技术
  - 时间同步口令，基于令牌与服务器的时间同步，并且采用国际标准时间，一般没60s产生一个新口令。
  - 事件同步，通过某一特定的事件次序及相同的种子值作为输入，通过哈希算法运算出一致的密码
  - 异步口令，主要采用挑战/应答（Challenge-Response）方式

动态口令：挑战-应答技术

1. C → S: userid; // 客户发送认证请求
2. S → C: r; // 服务器发送挑战，R为随机数
3. C → S: f(r||pwd); // f一般为哈希函数，pwd为C与S共享的长期密码
4. 收到客户的应答f(r||pwd)时，服务器可对r和pwd做同样的计算，如两者相同，则认证通过

- 注：pwd在认证过程中不以明文方式提交

访问控制

- 对通过认证的合法用户，其对系统资源的访问行为也需要依据安全策略进行控制
- 从系统资源安全保护的角度对访问进行授权控制
  - 主体：访问发起者，只要指用户，进程以及服务等
  - 客体：资源，主要指文件，目录等
  - 权限：对客体进行操作的许可，如读，写等
- 授权就是通过赋予主体一定的权限（读、写等），赋予客体一定的访问属性（读、写等），同时在主体与客体之间建立一套安全访问规则，实施主体访问客体的管理

访问控制

- 通过制定的安全访问机制，确保主体对客体的访问是经过授权的，同时要拒绝非授权的访问，以保证信息的**机密性，完整性和可用性**
  - 可用性？系统为合法用户持续提供服务的能力
    - 较难保证
- 即访问控制可提供机密性，完整性和可用性服务！

访问控制的二元关系描述

- 对主体设定的访问控制（规则）可用一个二元组（控制对象，访问类型）来表示
  - 控制对象：系统资源，如文件
  - 访问类型：对资源的访问，如读，写，执行等
- 二元组描述形式
  - 访问控制矩阵
  - 授权关系表
  - 访问能力表
  - 访问控制列表

访问控制矩阵

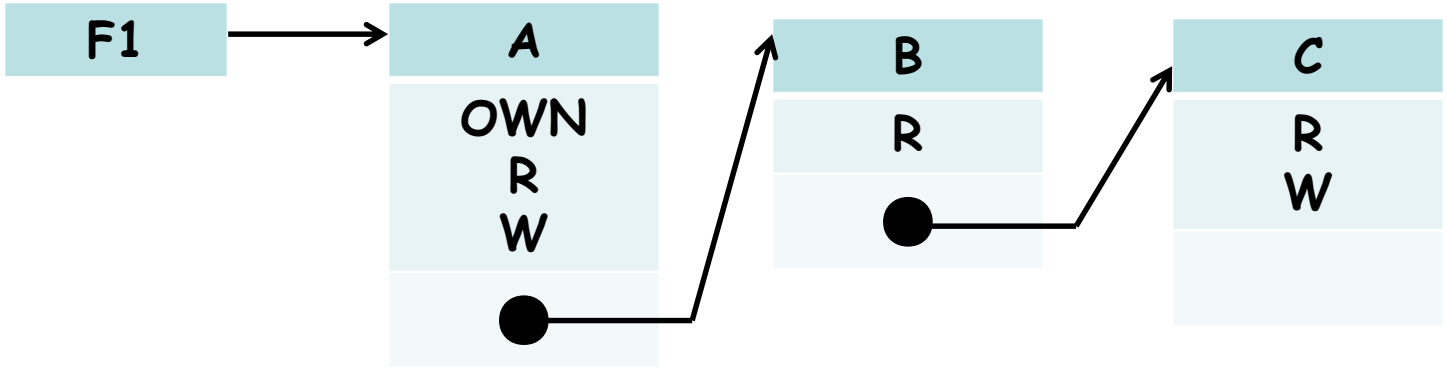
- 又称访问许可矩阵，它用行表示客体，列表示主体，在行列交叉处设定访问权限
- Own：所有权；R：读；W：写
- 例子：系统用户A，B和C，资源包括文件F1，F2和F3；下表表示系统的访问控制：

客体 主体	F1	F2	F3
A	OWN, R, W		OWN, R, W
B	R	OWN, R, W	W
B	R, W	R	

- 查表性能？稀疏矩阵?

访问控制列表 (Access Control List, ACL)

- 从客体出发描述控制信息，可以用对某一个资源指定任意一个用户的访问权限
- 例子：



自主、强制访问控制

- 在制定访问控制策略时，通常考虑资源所有权的概念
  - 资源的所有者，往往是资源的创建者
- 基于所有权的访问控制有两种策略
  - 自主访问控制，广泛应用在操作系统中
  - 强制访问控制，广泛应用在军事系统中

自主访问控制

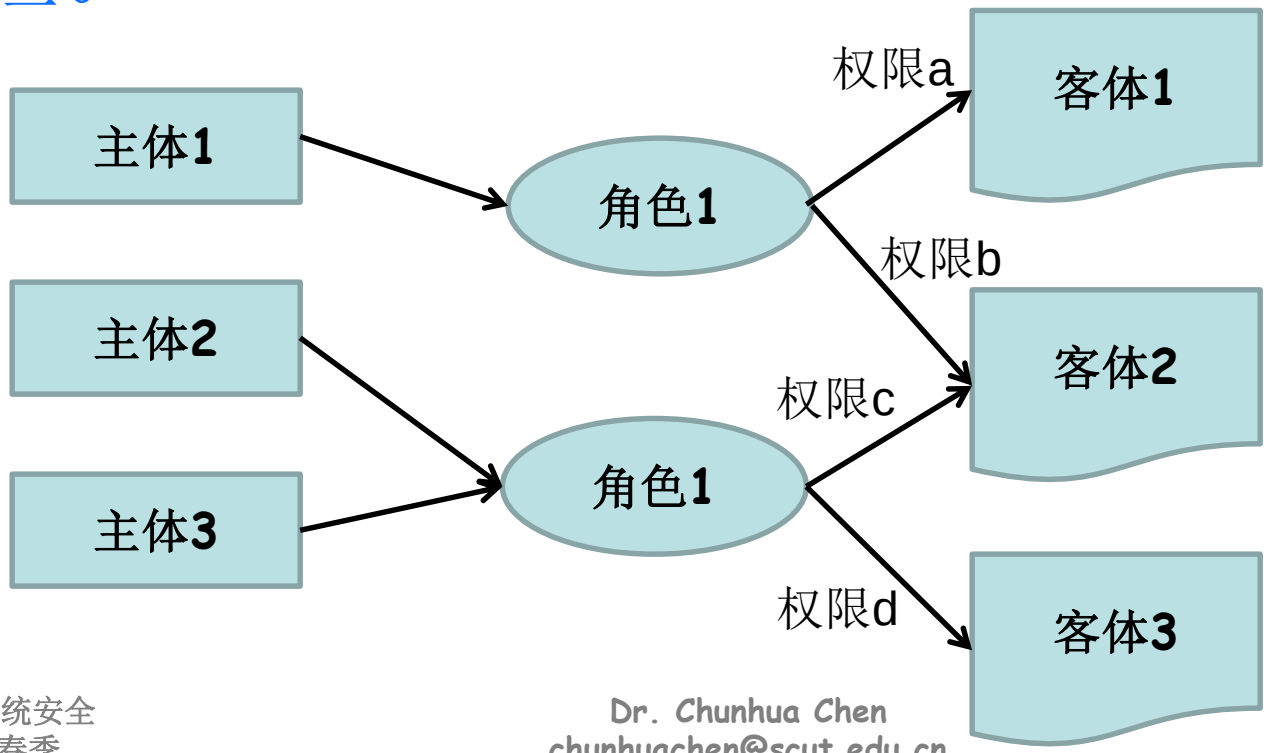
- 目前计算机系统中应用最广泛的一种策略，主流操作系统等均采用该策略
- 其基本思想是，资源的所有者可以对资源的访问进行控制，任意规定谁可以访问其资源，自主地直接或间接地将权限传给主体
  - 权限传递，灵活，但是也容易造成安全漏洞

强访问控制

- 其基本思想是系统要“强制”主体服从访问控制政策：系统（系统管理员）给主体和客体分配了不同的安全属性，用户不能改变自身或者任何客体的安全属性，即不允许单个用户确定访问权限，只有系统管理员才可以确定用户的访问权限。

基于角色的访问控制策略

- 角色是指一个组织或者任务中的岗位，职位或者分工。角色需要用户去扮演或者承担。



基于角色的访问控制策略

- 角色实际上是在主体（用户）和客体之间引入的中间控制机制层，实现权限与职责的分离；同时由于角色比个体用户具有较大的稳定性，极大地方便了权限管理

课程考核@Web安全

- 对一个典型Java Web应用
  - 安全审计：分析其脆弱性，潜在威胁，攻击手段
  - 安全机制：通信安全, 认证安全, 访问控制, 系统安全和其他
- Web应用涉及技术
  - HTML/CSS/JavaScript, JSP, Spring MVC 4 @ REST, Spring 4, MyBatis 3, Spring Security 4
  - MySQL 5

课程考核@Web安全

- 小组：4人一组
- 提交：程序，报告(会提供章节要求)
- 考核：现场演示系统, 回到老师问题

Further Reading: