Chapter 5 Authentication and Access Control

2017年3月22日 9:00

BY LSY
Outline:

- 认证 Authentication
- 授权 Authorization

2017/3/27 10:04
1.密码的实现

- 密文和明文信息不损失
- 但不保证密钥和密文信息不损失
  Early Unix Password, use DES as One-Way Hash Function:
  - Encrypt a NUL, and cut the password to 8 characters!
  - Artificial reduction: run DES 25 times!
  - Existing Problems:
    52 characters、10 numbers、32 symbols, password of 8 characters has: 94^8 ≈ 6 * 10^15 possible passwords
- Salting:
  - 前面加salt
  - salt + password —> hash 生成一个hash值
  - 验证时对hash进行验证
- Shadow:
  - /ete/passwd entry
  - /etc/shadow: only readable by system administrator (root)
  - 将文件分开
- add biometrics
- graphical passwords
- password guessing:
  - 尝试一些段密码，字典查询
  - 根据用户的信息
  - ....
- Biometric Identification
  - ad:
    - can't be stolen, lost or forgotten
  - dis:
    - cost of equipment\install\maintain
    - algorithm

2.Error rate of biometric identification

- fal

3.Network Authentication

- name
- name + IP ——fake IP
- name + IP + password ——截取password
- name + IP + password + encrypt ——replay

4.Kerberos
变成在客户端完成验证，不需要传输密码
存在时间有效性g

2017/3/29 8:18

1.Authorization

- basic access control
- basic function of verifying user identity;
- is needed to do deeper control

2.

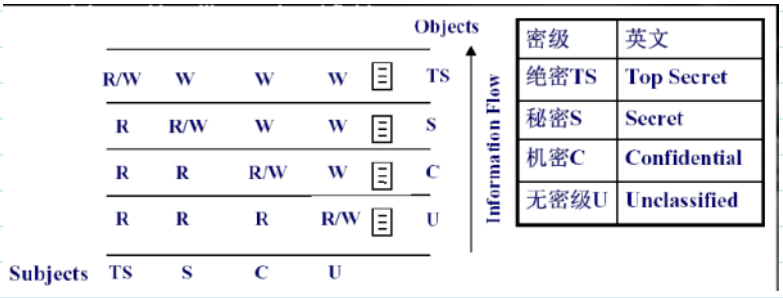
- subject: user or application process
- object: being accessed, such as files, programs, data
- privilege:

3.

- Three main functions : Authorization, Revoke, Checker
- Two stages : Make Policy, Execute Policy

4.

- DAC(Discretionary Access Control 自主访问控制)
  - discretionary 自己所拥有的权限可以自主赋予别人该权限
  - access control list: object连接subject
    capability list: subject连接object
    (用链表）
  - Unix OS
    - divide users into 3 categories
      -
      - User, u: owner
      - Group, g: belong to the same group with the file owner
      - Other, o: all other
    - divide the permission
      - Read, r
      - Write, w
      - Execute, x
    - 9 bits to indicate a file's access control list
      - 1~3 owner
      - 4~6 group
      - 7~9 other
      - RWX, 111, 7; RX, 101, 5; R, 100, 4
- MAC(Mandatory Access Control 强制访问控制)



  - Bell-LaPadula Model: Ensure confidentiality
    - Simple security property (No Read Up): 只能读安全级别一样或者低的
    - * property (No Write Down): 不能往下修改，以防泄露
  - Biba Model: Ensure integrity
    - 不能向下读，不能向上写
  - 不希望高级别信息向低级别泄露

    - covert channel:
        - resource exhaustion channel: 通过内存/资源来推理
        - load sensing channel: 对系统loading要求很高的程序来推断
    - coping with covert channel:
        - 关闭或者减速
        - 限制资源
        - 生成噪音（开资源然后再关闭，不断重复）
    - standard of MAC
        - C1: 访问控制
        - C2: 审计所有的访问控制都必须记录下来，包括用户登陆等
        - B1: 不允许自主访问，不需要考虑隐通道
        - B2: 最小特权，需要考虑隐通道
        - B3: 需要杯test/审核review/证明
        - A1：设计是可以被验证，需要形式化找到所有隐通道
- RBAC(role-based access control)
    - role: 角色，a group of users+a collection of operation permissions，多对多, 在不同情况下可以激活不同的permission
    - 最小特权原则
- 坏处
    - DAC 非常不灵活
    - DAC&MAC 成本很高

2017/4/1 10:10

- the principle of security access control
    - system administrator
    - security administrator
    - audit administrator

Review: